STIC Search Report
EIC 2100

STIC Database Tracking Number: 100755

TO:	From:
William C Vaughn **Location: PK2 5A52** **Art Unit : 2143** **Case Serial Number: 10014823**	**Carol Wong** **Location: EIC 2100** **PK2-4B33** **Phone: 305-9729** **carol.wong@uspto.gov**

Search Notes

Dear Examiner Vaughn,

Attached are the search results (from commercial databases) for your case.

Color tags mark the patents/articles which appear to be most relevant to the case.

Please call if you have any questions or suggestions for additional terminology, or a different approach to searching the case.

Thanks,
Carol

P.S. I left a voice mail for you and learned that you are out of the office until 8-22. However, I did not want to delay your search request until your return. The search results might not have the specific focus you need since we did not have an opportunity to discuss the case and your requirements. Also, I was unsure if 'address' is synonymous with 'id or identifier' of a server, so only the latter two terms were used. Please let me know if a refocused search would be useful for you.

STIC EIC 2100
Search Request Form

(99) 10055

Today's Date: 8/7/03

What date would you like to use to limit the search?
Priority Date: (29 Oct) 0 Other:

Name W. Vaughn
AU 2143 Examiner # 74926
Room # PK2 5A52 Phone 306-9129
Serial # 10014823

Format for Search Results (Circle One):
(PAPER) DISK EMAIL

Where have you searched so far?
(USP) (DWPI) (EPO) (JPO) ACM IBM TDB
IEEE INSPEC SPI Other _____

Is this a "Fast & Focused" Search Request? (Circle One) (YES) NO
A "Fast & Focused" Search is completed in 2-3 hours (maximum). The search must be on a very specific topic and meet certain criteria. The criteria are posted in EIC2100 and on the EIC2100 NPL Web Page at http://ptoweb/patents/stic/stic-tc2100.htm.

What is the topic, novelty, motivation, utility, or other specific details defining the desired focus of this search? Please include the concepts, synonyms, keywords, acronyms, definitions, strategies, and anything else that helps to describe the topic. Please attach a copy of the abstract, background, brief summary, pertinent claims and any citations of relevant art you have found.

obtaining a user's unique ID / along w/ an ID or identifier of a specific server w/in a group of servers. The servers authenticate a user based upon those two criterias:

- cookie
- ticket
- token
- key
- signature
- password

STIC Searcher Carol Wilson Phone 305-9729
Date picked up 8-18-03 Date Completed 8-19-03

Search and Information Resources Administration

```
File 348:EUROPEAN PATENTS 1978-2003/Aug W02
         (c) 2003 European Patent Office
File 349:PCT FULLTEXT 1979-2002/UB=20030814,UT=20030807
         (c) 2003 WIPO/Univentio
? ds

Set     Items   Description
S1     424000   ID OR IDS OR IDENTIFIER? OR IDENTIFIE? ? OR IDENTIFICATION?
              OR IDENTIFY?
S2      35249   S1(2N)(USER? ? OR ENDUSER? OR SUBSCRIBER? OR REQUEST?R? ? -
             OR MEMBER? ? OR PURCHASER? OR CLIENT? ? OR PARTICIPANT? OR BU-
             YER? ? OR PATRON? ? OR CONSUMER? ? OR CUSTOMER? OR SHOPPER?)
S3        731   USERID? ?
S4       9403   S1(2N)(SERVER? ? OR HOST? ? OR MAINFRAME? OR MAIN()FRAME? ?
              OR RAS) OR SERVERID? ? OR HOSTID? ?
S5     285142   AUTHENTICAT? OR VERIFIE? ? OR VERIFICAT? OR VERIFY? OR VAL-
             IDAT? OR AUTHORIS? OR AUTHORIZ? OR SUBSTANTIAT? OR CONFIRM?
S6      25180   S5(3N)(USER? ? OR ENDUSER? OR SUBSCRIBER? OR REQUEST?R? ? -
             OR MEMBER? ? OR PURCHASER? OR CLIENT? ? OR PARTICIPANT? OR BU-
             YER? ? OR PATRON? ? OR CONSUMER? ? OR CUSTOMER? OR SHOPPER?)
S7     156583   SERVER? ? OR HOST? ? OR MAINFRAME? OR MAIN()FRAME? ?
S8      30873   S7(3N)(GROUP??? ? OR COMMUNAL? OR COLLECTIVE? OR COMMUNITY
             OR SET OR SETS OR NETWORK? OR BLOC OR BLOCS OR BLOCK? ? OR CL-
             USTER? OR SERIES)
S9         59   MULTISERVER? OR MULTIHOST?
S10      9116   (MULTI OR MANY OR SEVERAL OR NUMEROUS OR PLURALIT? OR MULT-
             IPLE OR MULTITUD? OR CHAIN? OR NUMBER)(1W)S7
S11   1286796   ACCESS OR ACCESSE? ? OR ACCESSING OR REACCESS? OR LOGON? OR
              (LOG OR LOGS OR LOGGING)()(ON OR 'IN') OR LOGIN OR USE OR US-
             ES OR USAGE OR USING
S12      2029   S2:S3(S)S4
S13       340   S12(S)S6
S14     11247   IC=G06F-001
S15     14294   IC=G06F-015
S16     10541   IC=H04L-029
S17      5400   IC=H04L-009
S18       117   S13 AND S14:S17
S19        74   S18 AND S16:S17
S20        12   S13 AND S14:S15 AND S16:S17
S21        14   S13/TI,AB
S22     32346   (S1 OR KEY? ?)(3N)(MATCH? OR COMPAR? OR MAP OR MAPS OR MAP-
             PED OR MAPPING)
S23        65   S13(S)S22
S24        16   S23/TI,AB,CM
S25        97   S13(S)S8:S10
S26        34   S25(S)S22
S27        11   S26/TI,AB,CM
S28        15   S26 AND S14:S17
S29     57578   S11(3N)(NETWORK? ? OR LAN OR LANS OR WAN OR WANS OR NET()W-
             ORK? ? OR EXTRANET? OR INTERNET? OR INTRANET? OR WLAN? ? OR S-
             UBNET? OR VPN? ? OR MULTICOMPUTER?)
S30        16   S11(3N)SUB()(NET OR NETS)
S31         3   S19(3N)(WEB OR WEBSITE? OR WWW OR W3 OR NET OR WEBPAGE?)
S32        70   S13(S)S29:S31
S33        24   S32/TI,AB,CM
S34        24   S32 AND S14:S17
S35        51   S24 OR S27:S28 OR S33:S34
S36        44   S35 NOT S20:S21
S37        44   IDPAT (sorted in duplicate/non-duplicate order)
S38        44   IDPAT (primary/non-duplicate records only)
S39     24007   S11(3N)(WEB OR WEBSITE? OR WWW OR W3 OR NET OR WEBPAGE?)
```

S40	53	S13(S)S39
S41	14	S40/TI,AB,CM
S42	7	S40 AND S14:S17
S43	7	S41:S42 NOT (S20:S21 OR S38)
S44	7	IDPAT (sorted in duplicate/non-duplicate order)
S45	7	IDPAT (primary/non-duplicate records only)

20/5,K/6 (Item 1 from file: 349)

01016711 **Image available**

SYSTEM FOR PROVIDING CONTINUITY BETWEEN MESSAGING CLIENTS AND METHOD THEREFOR

SYSTEME POUR ASSURER LA CONTINUITE ENTRE PLUSIEURS CLIENTS DE MESSAGERIE ET PROCEDE CORRESPONDANT

Patent Applicant/Assignee:
MOTOROLA INC, 1303 East Algonquin Road, Schaumburg, IL 60196, US, US (Residence), US (Nationality)

Inventor(s):
EATON Eric Thomas, 3198 Medinah Circle, Lake Worth, FL 33467, US,
HAYES David J, 7544 Wentworth Drive, Lake Worth, FL 33467, US,
MOCK Von Alan, 8114 Rose Marie Circle, Boynton Beach, FL 33437, US,

Legal Representative:
DULANEY Randi L (et al) (agent), 8000 West Sunrise Blvd., Rm 1610, Fort Lauderdale, FL 33322, US,

Patent and Priority Information (Country, Number, Date):
Patent: WO 200346726 A1 20030605 (WO 0346726)
Application: WO 2002US37910 20021125 (PCT/WO US0237910)
Priority Application: US 2001995338 20011127

Designated States: AE AG AL AM AT AU AZ BA BB BG BR BY BZ CA CH CN CO CR CU CZ DE DK DM DZ EC EE ES FI GB GD GE GH GM HR HU ID IL IN IS JP KE KG KP KR KZ LC LK LR LS LT LU LV MA MD MG MK MN MW MX MZ NO NZ OM PH PL PT RO RU SD SE SG SI SK SL TJ TM TN TR TT TZ UA UG UZ VC VN YU ZA ZM ZW
(EP) AT BE BG CH CY CZ DE DK EE ES FI FR GB GR IE IT LU MC NL PT SE SK TR
(OA) BF BJ CF CG CI CM GA GN GQ GW ML MR NE SN TD TG
(AP) GH GM KE LS MW MZ SD SL SZ TZ UG ZM ZW
(EA) AM AZ BY KG KZ MD RU TJ TM

Main International Patent Class: G06F-011/30
International Patent Class: G06F-012/14; **G06F-015/16** ; **H04L-009/00** ; **H04L-009/32**
Publication Language: English
Filing Language: English
Fulltext Availability:
Detailed Description
Claims
Fulltext Word Count: 28416

English Abstract
A messaging communication system (10) includes a plurality of messaging clients (12). A first messaging client (14) establishes a first communication connection (16) operating using a plurality of client data (25). The first messaging client (14) transfers the plurality of client data (25) to a second messaging client (20). The second messaging client (20) establishes a second communication connection (22) operating using the plurality of client data (25).

French Abstract
Un systeme de communication a messagerie (10) comprend plusieurs clients de messagerie (12). Un premier client de messagerie (14) etablit une premiere connexion de communication (16) fonctionnant avec plusieurs elements de donnees client (25). Ledit premier client de messagerie (14) transfere ces plusieurs elements de donnees client (25) a un deuxieme client de messagerie (20). Le deuxieme client de messagerie (20) etablit une deuxieme connexion de communication (22) fonctionnant avec plusieurs elements de donnees client (25).

Legal Status (Type, Date, Text)
Publication 20030605 A1 With international search report.

...International Patent Class: **G06F-015/16** ...

... **H04L-009/00** ...

... **H04L-009/32**
Fulltext Availability:
Detailed Description

Detailed Description
... data 25 can include any of the client data mentioned herein or an equivalent.

The **client** version **identifier** is preferably the name ...which a message server is utilized to manage the plurality of messaging sessions 24, the **server identifier** 32 **identifies** the message **server** . For example, the **server identifier** 32 can be a wireless address, an IP (internet protocol) address, or an IP address 33 preferably includes a code that is used to **authenticate** the account **user** 30 to the messaging communication system 10. For example, the authentication key 33 could be...
? t20/5/7

20/5/7 (Item 2 from file: 349)
DIALOG(R)File 349:PCT FULLTEXT
(c) 2003 WIPO/Univentio. All rts. reserv.

01008594 **Image available**
ENHANCED QUALITY OF IDENTIFICATION IN A DATA COMMUNICATIONS NETWORK
AMELIORATION DE LA QUALITE D'IDENTIFICATION DANS UN RESEAU DE TRANSMISSION DE DONNEES
Patent Applicant/Assignee:
SUN MICROSYSTEMS INC, 4120 Network Circle, Santa Clara, CA 95054, US, US (Residence), US (Nationality)
Inventor(s):
DE JONG Eduard K, 522 S. Fremont, San Mateo, CA 94402, US,
LEVY Moshe, 1512 Klamath Drive, Sunnyvale, CA 94087, US,
LEUNG Albert Y, 4175 Orin Court, San Jose, CA 95110, US,
Legal Representative:
RITCHIE David B (et al) (agent), Thelen Reid & Priest LLP, P.O. Box 640640, San Jose, CA 95164-0640, US,
Patent and Priority Information (Country, Number, Date):
Patent: WO 200338579 A1 20030508 (WO 0338579)
Application: WO 2002US34713 20021029 (PCT/WO US0234713)
Priority Application: US 200114823 20011029
Designated States: AE AG AL AM AT AU AZ BA BB BG BR BY BZ CA CH CN CO CR CU CZ DE DK DM DZ EC EE ES FI GB GD GE GH GM HR HU ID IL IN IS JP KE KG KP KR KZ LC LK LR LS LT LU LV MA MD MG MK MN MW MX MZ NO NZ OM PH PL PT RO RU SD SE SG SI SK SL TJ TM TN TR TT TZ UA UG UZ VC VN YU ZA ZM ZW
(EP) AT BE BG CH CY CZ DE DK EE ES FI FR GB GR IE IT LU MC NL PT SE SK TR
(OA) BF BJ CF CG CI CM GA GN GQ GW ML MR NE SN TD TG
(AP) GH GM KE LS MW MZ SD SL SZ TZ UG ZM ZW
(EA) AM AZ BY KG KZ MD RU TJ TM
Main International Patent Class: **G06F-001/00**
International Patent Class: **H04L-029/06**
Publication Language: English
Filing Language: English
Fulltext Availability:

Detailed Description
Claims
Fulltext Word Count: 21515

English Abstract
A method for enhanced quality of identification in a data communications network includes obtaining a **user identifier** that includes an **identification server ID** and an identification randomized **ID** . The **identification server ID identifies** an **identification server** peer group. The **identification server** peer group includes at least one server that maintains a mapping between an identification randomized **ID** and a **user authentication** peer group capable of **authenticating** a **user** associated with a particular randomized ID, and a mapping between the identification randomized **ID** and **user** information. The method also includes requesting **authorization** of the **user** by presenting the **user identifier** to a corresponding **identification server** peer group. Each **server** in the **identification server** peer group is configured to search for one or more matching entries including the randomized ID.

French Abstract
L'invention porte sur un procede ameliorant la qualite d'identification dans un reseau de transmission de donnees consistant a obtenir un identificateur d'utilisateur comprenant un ID d'identification de serveur et un ID d'identification pris au hasard. L'ID d'identification de serveur identifie un groupe de serveurs prestataires de services comportant au moins un serveur contenant: une correspondance entre l'ID d'identification pris au hasard et un groupe pair d'identification de l'utilisateur pouvant authentifier un utilisateur associe a un ID d'identification pris au hasard particulier, et une correspondance entre l'ID d'identification pris au hasard et une information utilisateur. Le procede consiste egalement a requerir l'autorisation de l'utilisateur en presentant l'identificateur d'utilisateur a un groupe de serveurs pairs d'identification correspondant. Chacun des serveurs dudit groupe est concu pour rechercher une ou plusieurs occurrences correspondantes dont l'ID pris au hasard.

Legal Status (Type, Date, Text)
Publication 20030508 A1 With international search report.
Examination 20030710 Request for preliminary examination prior to end of 19th month from priority date
? t20/5,k/11

20/5,K/11 (Item 6 from file: 349)

00785113 **Image available**
VIRTUAL SMART CARD SYSTEM AND METHOD
SYSTEME A CARTE A PUCE VIRTUELLE ET PROCEDE D'UTILISATION
Patent Applicant/Assignee:
SECURE COMPUTING CORPORATION, 2675 Long Lake Road, Roseville, MN 55113, US, US (Residence), US (Nationality)
Inventor(s):
SMITH Lawrence, 3620 Concord Boulevard, Concord, CA 94519, US,
LEVENBERG Richard, 3346 Helen Lane, Lafayette, CA 94549, US,
Legal Representative:
VIKSNINS Ann S (et al) (agent), Schwegman, Lundberg, Woessner & Kluth, P.O. Box 2938, Minneapolis, MN 55402, US,
Patent and Priority Information (Country, Number, Date):

Patent: WO 200118635 A2-A3 20010315 (WO 0118635)
Application: WO 2000US24352 20000901 (PCT/WO US0024352)
Priority Application: US 99389540 19990903
(EP) AT BE CH CY DE DK ES FI FR GB GR IE IT LU MC NL PT SE
Main International Patent Class: **G06F-001/00**
International Patent Class: **H04L-029/06**
Publication Language: English
Filing Language: English
Fulltext Availability:
Detailed Description
Claims
Fulltext Word Count: 4934

English Abstract
A public key authentication system and method for use in a computer system having a plurality of users. The system includes a virtual smart card server, storage connected to the virtual smart card server, and a virtual smart card agent connected to the virtual smart card server. The storage includes a plurality of virtual smart cards, wherein each virtual smart card is associated with a user and wherein each smart card includes a private key. The virtual smart card agent authenticates the user and accesses the authenticated user's virtual smart card to obtain the user's private key.

French Abstract
L'invention concerne un systeme d'authentification a cles publiques et son procede d'utilisation dans un systeme informatique comprenant plusieurs utilisateurs. Le systeme comprend un serveur a carte a puce virtuelle, une memoire connectee au serveur a carte a puce virtuelle, et un agent a carte a puce virtuelle connecte au serveur a carte a puce virtuelle. La memoire comprend plusieurs cartes a puce virtuelles. Chaque carte a puce virtuelle est associee a un utilisateur et comprend une cle privee. L'agent a carte a puce virtuelle authentifie l'utilisateur et accede a la carte a puce virtuelle de l'utilisateur authentifie pour obtenir la cle privee de l'utilisateur.

Legal Status (Type, Date, Text)
Publication 20010315 A2 Without international search report and to be republished upon receipt of that report.
Examination 20010614 Request for preliminary examination prior to end of 19th month from priority date
Search Rpt 20011213 Late publication of international search report
Republication 20011213 A3 With international search report.

Main International Patent Class: **G06F-001/00**
International Patent Class: **H04L-029/06**
Fulltext Availability:
Detailed Description
Claims

Detailed Description
... includes a plurality of public keys, wherein each public key is associated with a unique **user identifier** . The **host** system includes a public key **authentication client** and an interface to a smart-card-enabled application, wherein the public key **authentication client** is connected to the authentication server. The public key **authentication client** receives a challenge issued by the authentication server, signs the challenge with a digital signature...

Claim

... includes a plurality of public keys, wherein each public key is associated with a unique **user identifier** ; and
a **host** system, wherein the host system includes a public key
1 5 **authentication client** and an interface to a smart-card-enabled application, wherein the public key **authentication client** is connected to the authentication
server;
wherein the public key **authentication client** receives a challenge issued
by the authentication server, signs the challenge with a digital signature...

21/5,K/4 (Item 4 from file: 348)
DIALOG(R)File 348:EUROPEAN PATENTS

00934787
Secure two-piece user authentication in a computer network
Gesicherte zweiteilige Benutzer-Authentifizierung in einem Rechnernetz
Authentification en deux pieces securisee d'un utilisateur dans un reseau d'ordinateurs
PATENT ASSIGNEE:
Compaq Computer Corporation, (687792), 20555 S.H. 249, Houston Texas 77070, (US), (applicant designated states: AT;BE;CH;DE;DK;ES;FI;FR;GB;GR;IE;IT;LI;LU;MC;NL;PT;SE)
INVENTOR:
Angelo, Michael F., 14926 Walters Road, Houston, Texas 77068, (US)
Olarig, Sompong P., 15415 Evergreen Knoll Lane, Cypress, Texas 77429, (US)
LEGAL REPRESENTATIVE:
Brunner, Michael John et al (28871), GILL JENNINGS & EVERY Broadgate House 7 Eldon Street, London EC2M 7LH, (GB)
PATENT (CC, No, Kind, Date): EP 851335 A2 980701 (Basic)
EP 851335 A3 990616
APPLICATION (CC, No, Date): EP 97310653 971230;
PRIORITY (CC, No, Date): US 774809 961231
DESIGNATED STATES: DE; FR; GB
INTERNATIONAL PATENT CLASS: G06F-001/00;

ABSTRACT EP 851335 A2
A computer system according to the present invention utilizes a two-piece authentication procedure to securely provide **user authentication** over a network. In the disclosed embodiment of the invention, a user password is entered during a secure power-up procedure. The user password is encrypted by an external token or smart card that stores an encryption algorithm furnished with an encryption key that is unique or of limited production. A network password is thereby created. The network password is maintained in a secure memory space such as System Management Mode (SMM) memory. When the user desires to access a network resource such as a hard drive in a server, the network password is encrypted and communicated over the network. In the case of a server hard drive, the network password is encrypted using the servers public key (or another key that is known to the **server**). Optional node lidentification information is appended to the network password prior to communication over the network. The node identification information can be used for a variety of purposes, including limiting access to certain pieces of data to specified users on specified machines. Once received by the server, the encrypted network password is decrypted using the servers public key. A **user verification** process is then performed on the network password to determine which, if any, access privileges have been accorded the network user. Numerous other uses for the network password are disclosed, and permit the network resources to be securely compartmentalized with the option to have multiple user levels. The two-piece nature of the authentication process assures that if either the user password or the external token is stolen, it is of little value. Both pieces are required to access protected resources and uniquely lidentify a **user** to the network. Further, a network users identity is maintained when working on different machines.
ABSTRACT WORD COUNT: 306

LEGAL STATUS (Type, Pub Date, Kind, Text):
 Examination: 020918 A2 Date of dispatch of the first examination report: 20020731
 Examination: 20000202 A2 Date of request for examination: 19991206
 Application: 980701 A2 Published application (A1with Search Report ;A2without Search Report)
 Search Report: 990616 A3 Separate publication of the European or International search report
LANGUAGE (Publication,Procedural,Application): English; English; English
FULLTEXT AVAILABILITY:

Available Text	Language	Update	Word Count
CLAIMS A	(English)	9827	840
SPEC A	(English)	9827	6236
Total word count - document A			7076
Total word count - document B			0
Total word count - documents A + B			7076

...ABSTRACT system according to the present invention utilizes a two-piece authentication procedure to securely provide **user authentication** over a network. In the disclosed embodiment of the invention, a user password is entered...

...is encrypted using the servers public key (or another key that is known to the **server**). Optional node **identification** information is appended to the network password prior to communication over the network. The node ...

...by the server, the encrypted network password is decrypted using the servers public key. A **user verification** process is then performed on the network password to determine which, if any, access privileges...

...it is of little value. Both pieces are required to access protected resources and uniquely **identify** a **user** to the network. Further, a network users identity is maintained when working on different machines.
? t21/5/7,t21/5,k/11-12
>>>'T21' not recognized as item list
? t21/5/7

21/5/7 (Item 1 from file: 349)
DIALOG(R)File 349:PCT FULLTEXT
(c) 2003 WIPO/Univentio. All rts. reserv.

01008594 **Image available**
ENHANCED QUALITY OF IDENTIFICATION IN A DATA COMMUNICATIONS NETWORK
AMELIORATION DE LA QUALITE D'IDENTIFICATION DANS UN RESEAU DE TRANSMISSION DE DONNEES
Patent Applicant/Assignee:
  SUN MICROSYSTEMS INC, 4120 Network Circle, Santa Clara, CA 95054, US, US (Residence), US (Nationality)
Inventor(s):
  DE JONG Eduard K, 522 S. Fremont, San Mateo, CA 94402, US,
  LEVY Moshe, 1512 Klamath Drive, Sunnyvale, CA 94087, US,
  LEUNG Albert Y, 4175 Orin Court, San Jose, CA 95110, US,
Legal Representative:
  RITCHIE David B (et al) (agent), Thelen Reid & Priest LLP, P.O. Box 640640, San Jose, CA 95164-0640, US,
Patent and Priority Information (Country, Number, Date):
  Patent: WO 200338579 A1 20030508 (WO 0338579)
  Application: WO 2002US34713 20021029 (PCT/WO US0234713)
  Priority Application: US 200114823 20011029
Designated States: AE AG AL AM AT AU AZ BA BB BG BR BY BZ CA CH CN CO CR CU

CZ DE DK DM DZ EC EE ES FI GB GD GE GH GM HR HU ID IL IN IS JP KE KG KP
KR KZ LC LK LR LS LT LU LV MA MD MG MK MN MW MX MZ NO NZ OM PH PL PT RO
RU SD SE SG SI SK SL TJ TM TN TR TT TZ UA UG UZ VC VN YU ZA ZM ZW
(EP) AT BE BG CH CY CZ DE DK EE ES FI FR GB GR IE IT LU MC NL PT SE SK TR
(OA) BF BJ CF CG CI CM GA GN GQ GW ML MR NE SN TD TG
(AP) GH GM KE LS MW MZ SD SL SZ TZ UG ZM ZW
(EA) AM AZ BY KG KZ MD RU TJ TM
Main International Patent Class: G06F-001/00
International Patent Class: H04L-029/06
Publication Language: English
Filing Language: English
Fulltext Availability:
Detailed Description
Claims
Fulltext Word Count: 21515

English Abstract
A method for enhanced quality of identification in a data communications network includes obtaining a **user identifier** that includes an **identification server ID** and an identification randomized **ID** . The **identification server ID identifies** an **identification server** peer group. The **identification server** peer group includes at least one server that maintains a mapping between an identification randomized **ID** and a **user** authentication peer group capable of **authenticating** a **user** associated with a particular randomized ID, and a mapping between the identification randomized **ID** and **user** information. The method also includes requesting **authorization** of the **user** by presenting the **user identifier** to a corresponding **identification server** peer group. Each **server** in the **identification server** peer group is configured to search for one or more matching entries including the randomized ID.

French Abstract
L'invention porte sur un procede ameliorant la qualite d'identification dans un reseau de transmission de donnees consistant a obtenir un identificateur d'utilisateur comprenant un ID d'identification de serveur et un ID d'identification pris au hasard. L'ID d'identification de serveur identifie un groupe de serveurs prestataires de services comportant au moins un serveur contenant: une correspondance entre l'ID d'identification pris au hasard et un groupe pair d'identification de l'utilisateur pouvant authentifier un utilisateur associe a un ID d'identification pris au hasard particulier, et une correspondance entre l'ID d'identification pris au hasard et une information utilisateur. Le procede consiste egalement a requerir l'autorisation de l'utilisateur en presentant l'identificateur d'utilisateur a un groupe de serveurs pairs d'identification correspondant. Chacun des serveurs dudit groupe est concu pour rechercher une ou plusieurs occurrences correspondantes dont l'ID pris au hasard.

Legal Status (Type, Date, Text)
Publication 20030508 A1 With international search report.
Examination 20030710 Request for preliminary examination prior to end of 19th month from priority date
? t21/5,k/11-12

21/5,K/11 (Item 5 from file: 349)
DIALOG(R)File 349:PCT FULLTEXT

00811460 **Image available**

SECURE GATEWAY HAVING USER IDENTIFICATION AND PASSWORD AUTHENTICATION
PASSERELLE SECURISEE POSSEDANT DES FONCTIONS D'IDENTIFICATION UTILISATEUR ET D'AUTHENTIFICATION DU MOT DE PASSE

Patent Applicant/Assignee:
GTE SERVICE CORPORATION, 600 Hidden Ridge Drive, Irving, TX 75038, US, US (Residence), US (Nationality)
Inventor(s):
GRANTGES David R Jr, 1620 Rio Circle, Clearwater, FL 33764, US,
Legal Representative:
SUCHYTA Leonard C (agent), c/o Christian R. Andersen, 600 Hidden Ridge Drive, Mailcode HQE03G13, Irving, TX 75038, US,
Patent and Priority Information (Country, Number, Date):
Patent: WO 200145049 A1 20010621 (WO 0145049)
Application: WO 2000US33816 20001214 (PCT/WO US0033816)
Priority Application: US 99170686 19991214; US 99471901 19991223
Designated States: AE AG AL AM AT AT (utility model) AU AZ BA BB BG BR BY BZ CA CH CN CR CU CZ CZ (utility model) DE DE (utility model) DK DK (utility model) DM DZ EE EE (utility model) ES FI FI (utility model) GB GD GE GH GM HR HU ID IL IN IS JP KE KG KP KR KZ LC LK LR LS LT LU LV MA MD MG MK MN MW MX MZ NO NZ PL PT RO RU SD SE SG SI SK SK (utility model) SL TJ TM TR TT TZ UA UG UZ VN YU ZA ZW
(EP) AT BE CH CY DE DK ES FI FR GB GR IE IT LU MC NL PT SE TR
(OA) BF BJ CF CG CI CM GA GN GW ML MR NE SN TD TG
(AP) GH GM KE LS MW MZ SD SL SZ TZ UG ZW
(EA) AM AZ BY KG KZ MD RU TJ TM
Main International Patent Class: G06T-011/30
International Patent Class: H02L-009/00
Publication Language: English
Filing Language: English
Fulltext Availability:
Detailed Description
Claims
Fulltext Word Count: 9948

English Abstract
A computer system (20) for **authenticated** access for a **client** (18) over an insecure network (32) to secure a destination server (24) on another network, through the use of a **client authentication** certificate (50). A proxy server (40) intercepts messages destined for the destination server (24), and forwards the intercepted messages to a gateway (38) on the network (20). The gateway (38) configures a cookie, with identifiers (48) sufficient to **identify** the destination **server** (24), or alternatively, utilizes a **user** (18) **identification** and password.

French Abstract
L'invention concerne un systeme informatique (20) destine a fournir a un client (18) d'un reseau (32) non securise un acces authentifie a un serveur (24) de destination d'un reseau securise, via l'utilisation d'un certificat (50) d'authentification client. A cet effet, un serveur mandataire (40) intercepte les messages destines au serveur (24) de destination, et transmet les messages interceptes a une passerelle (38) du reseau (20). La passerelle (38) configure un temoin, avec des identificateurs (48) suffisants pour identifier le serveur (24) de destination, ou alors elle utilise une identification utilisateur (18) et un mot de passe.

Legal Status (Type, Date, Text)
Publication 20010621 A1 With international search report.
Examination 20011025 Request for preliminary examination prior to end of 19th month from priority date

Correction 20020103 Corrections of entry in Section 1: under (30) replace "15 December 1999 (15.12.99)" by "14 December 1999 (14.12.99)"
Republication 20020103 A1 With international search report.

English Abstract
A computer system (20) for **authenticated** access for a **client** (18) over an insecure network (32) to secure a destination server (24) on another network, through the use of a **client authentication** certificate (50). A proxy server (40) intercepts messages destined for the destination server (24), and...

...on the network (20). The gateway (38) configures a cookie, with identifiers (48) sufficient to **identify** the destination **server** (24), or alternatively, utilizes a **user** (18) **identification** and password.

21/5,K/12 (Item 6 from file: 349)
DIALOG(R)File 349:PCT FULLTEXT

00811372 **Image available**
SECURE GATEWAY HAVING ROUTING FEATURE
PASSERELLE SECURISEE A CARACTERISTIQUE D'ACHEMINEMENT
Patent Applicant/Assignee:
GTE SERVICE CORPORATION, 600 Hidden Ridge Drive, Irving, TX 75038, US, US (Residence), US (Nationality)
Inventor(s):
GRANTGES David R Jr, 1620 Rio Circle, Clearwater, FL 33764, US,
MCGRATH Lawrence R, 8134 Natures Way #11, Bradenton, FL 34202, US,
Legal Representative:
SUCHYTA Leonard C (agent), c/o Christian R. Andersen, 600 Hidden Ridge Drive, Mailcode HQE03G13, Irving, TX 75038, US,
Patent and Priority Information (Country, Number, Date):
Patent: WO 200144951 A1 20010621 (WO 0144951)
Application: WO 2000US33813 20001214 (PCT/WO US0033813)
Priority Application: US 99170686 19991214; US 99471645 19991223
Designated States: AE AG AL AM AT AT (utility model) AU AZ BA BB BG BR BY BZ CA CH CN CR CU CZ CZ (utility model) DE DE (utility model) DK DK (utility model) DM DZ EE EE (utility model) ES FI FI (utility model) GB GD GE GH GM HR HU ID IL IN IS JP KE KG KP KR KZ LC LK LR LS LT LU LV MA MD MG MK MN MW MX MZ NO NZ PL PT RO RU SD SE SG SI SK SK (utility model) SL TJ TM TR TT TZ UA UG UZ VN YU ZA ZW
(EP) AT BE CH CY DE DK ES FI FR GB GR IE IT LU MC NL PT SE TR
((OAPI utility model)) BF BJ CF CG CI CM GA GN GW ML MR NE SN TD TG
(AP) GH GM KE LS MW MZ SD SL SZ TZ UG ZW
(EA) AM AZ BY KG KZ MD RU TJ TM
Main International Patent Class: G06F-012/14
International Patent Class: G06F-013/00; G06F-017/30
Publication Language: English
Filing Language: English
Fulltext Availability:
Detailed Description
Claims
Fulltext Word Count: 9825

English Abstract
A computer system provides **authenticated** access for a **client** computer (18) over an insecure, public network (26) to one of a plurality of destination servers (28) on private, secure network, through the use of a client-side X.509 digital certificate. A firewall (32) is disposed

between the insecure, public network (26) and the private network. A demilitarized zone (DMZ) proxy server (34) intercepts messages destined for the destination servers (28), and forwards the intercepted messages through the firewall (32) to a gateway (38) on the private network. The gateway (38) is configured to create a cookie, based on the selection of one of several applications (30) available on the private network. The cookie contains an identifier sufficient to **identify** the destination **server** (28) corresponding to the selected application (30). Messages from the client computer include the cookie. The gateway (38) processes the cookie and appends the identifier on a destination URL portion of the messages for routing. An alternate computer system **authenticates** a **user** of a remote client computer on the insecure network site (26) of the firewall (32) using a **user identification** and password.

French Abstract
La presente invention concerne un systeme informatique qui fournit a un ordinateur de client (18), sur un reseau public non securise (26), un acces authentifie a un ou plusieurs serveurs de destination (28), sur un reseau prive securise, par utilisation d'un certificat numerique X.509 cote client. Un pare-feu (32) est place entre le reseau public non securise (26) et le reseau prive. Un serveur mandataire de zone demilitarisee (DMZ) (34) intercepte des messages destines aux serveurs de destination (28) et les retransmet, a travers le pare-feu (32), a une passerelle (38) sur le reseau prive. Cette passerelle (38) est configuree pour creer un temoin, sur la base de la selection d'une de plusieurs applications (30), qui sont disponibles sur le reseau prive. Ce temoin contient un identificateur qui permet d'identifier le serveur de destination (28) correspondant a l'application selectionnee (30). Des messages issus de l'ordinateur de client comprennent le temoin. La passerelle (38) traite le temoin et ajoute l'identificateur a une partie d'adresse URL de destination des messages en vue d'un acheminement. Un systeme informatique alterne authentifie un utilisateur d'ordinateur de client eloigne, sur le site (26) de reseau non securise du pare-feu (32), par utilisation d'une identification et d'un mot de passe d'utilisateur.

Legal Status (Type, Date, Text)
Publication 20010621 A1 With international search report.
Examination 20011025 Request for preliminary examination prior to end of 19th month from priority date

English Abstract
A computer system provides **authenticated** access for a **client** computer (18) over an insecure, public network (26) to one of a plurality of destination...

...several applications (30) available on the private network. The cookie contains an identifier sufficient to **identify** the destination **server** (28) corresponding to the selected application (30). Messages from the client computer include the cookie...

...identifier on a destination URL portion of the messages for routing. An alternate computer system **authenticates** a **user** of a remote client computer on the insecure network site (26) of the firewall (32) using a **user identification** and password.
?

38/5,K/36 (Item 36 from file: 349)
DIALOG(R)File 349:PCT FULLTEXT

00766059 **Image available**
QUERY INTERFACE TO POLICY SERVER
INTERFACE D'INTERROGATION VERS SERVEUR DE REGLES
Patent Applicant/Assignee:
INTERNET DYNAMICS INC, 3717 E. Thousand Oaks Boulevard, Westlake Village, CA 91362, US, US (Residence), US (Nationality), (For all designated states except: US)
Patent Applicant/Inventor:
HANNEL Clifford Lee, 3178 Futura Point, Thousand Oaks, CA 91362, US, US (Residence), US (Nationality), (Designated only for: US)
MAY Anthony Allan, 6644 Glade Avenue #217, Woodland Hills, CA 91303, US, US (Residence), CA (Nationality), (Designated only for: US)
Legal Representative:
NELSON Gordon E, 57 Central Street, P.O. Box 782, Rowley, MA 01969, US
Patent and Priority Information (Country, Number, Date):
Patent: WO 200079434 A1 20001228 (WO 0079434)
Application: WO 2000US17078 20000621 (PCT/WO US0017078)
Priority Application: US 99140417 19990622
Designated States: AU JP SG US
(EP) AT BE CH CY DE DK ES FI FR GB GR IE IT LU MC NL PT SE
Main International Patent Class: G06F-017/30
Publication Language: English
Filing Language: English
Fulltext Availability:
Detailed Description
Claims
Fulltext Word Count: 54190

English Abstract
A scalable access filter that is used together with others like it in a virtual private network to control access by users at clients in the network to information resources provided by servers in the network. Each access filter use a local copy of an access control data base (3845) to determine whether an access request is made by a user. Each user belongs to one or more user groups and each information ressource belongs to one or more information sets. Access is permitted or denied according to access policies which define access in terms of the user groups and information sets. The first access filter in the path performs the access check, encrypts and authenticates the request; the other access filters in the path do not repeat the access check. The interface used by applications to determine whether a user has access to an entity is now an SQL query. The policy server (3811) assembles the information needed for the response to the query from various information sources, including source external to the policy server.

French Abstract
L'invention concerne un filtre d'acces scalaire utilise avec d'autres filtres similaires dans un reseau prive virtuel afin de controler l'acces des utilisateurs a des clients du reseau pour obtenir des ressources d'informations fournies par des serveurs sur le reseau. Chaque filtre d'acces utilise une copie locale d'une base de donnees de controle d'acces (3845) pour determiner si la demande d'acces est effectuee par un utilisateur. Chaque utilisateur appartient a au moins un groupe d'utilisateurs et chaque ressource d'informations appartient a au moins un ensemble d'informations. L'acces est autorise ou refuse en fonction des politiques d'acces qui definissent l'acces en terme des groupes

d'utilisateurs et des ensembles d'informations. Le premier filtre d'acces dans la voie effectue la verification d'acces, decrypte, et authentifie la demande, les autres filtres d'acces dans la voie ne repetent pas la verification d'acces. L'interface utilisee par les applications pour determiner si un utilisateur a acces a une entite est alors une demande SQL. Le serveur de regles (3811) assemble les informations requises pour la reponse a la demande emanant de plusieurs sources d'informations, y compris une source externe audit serveur.

Legal Status (Type, Date, Text)
Publication 20001228 A1 With international search report.
Examination 20010802 Request for preliminary examination prior to end of 19th month from priority date

Fulltext Availability:
Claims

Claim
... ACCESS FILTER ACCESS FILTER FM
203 ml 2QM
De fft-- C, in
301 301 CLIENTS **SERVER**
Fr 7- INFORMATION **SET** 2190)
ffwt- 219(k)
Fig* 2 F7@ 201
ffk I FA
POLICY 303
ADMIN. POLICY...

...Alert lo Emerqenc
9 y
911 Main- --- User Groups Resource Sets Policy Sm art Filter
Servers : - **Networks** I Net Security JAIert Setup I Optior
ab for details
(D Ed: Default Values 0...an
allow or deny policy. DBUsersTreeFile Describes the user groups tree as a flattened array. **Maps** each
DB UserGroup **ID** to a list of UserGroupIDs for parent user groups
DBResourcesFile 23og Describes policy application from...

...flattened array. Maps
each DB ResourceGroupll) to a list of ResourceGroupiDs for parent information sets,
User Identification Information 2@311
DBIPRangesFile IP Ranges data. Maps from IPRangeDefID to the IP range data...

...IP domain data. DBCertificatesFile Certificate data. Maps from
CertificateDeflD to the certificate data.
DBWindowslDFile Windows **ID** data. **Maps** from WindowDefID to the windows ID
data. DBSmartCardlDFile Smart card (authentication token) data. Maps from ...

...user groups. Maps from certificate data
File to UserGrouplDs. 21-0,1
DBWindowsIDByUserGroup Relates Windows **IDs** to **user** groups. **Maps** from Windows **ID** File data to UserGrouplDs. DBSmartCardIDByUser Relates Smart Card (**authentication** token) data to **user** groups.
GroupFile Maps from authentication token data to UserGrouplDs

2301
Fig. 23A
MMF File Name...

...DBResourcesByServerlDFile Relates servers to resources. Maps from ServerlDs to
ResourcelDs for resources held on the **server identified** by the **ServerID** . DBResourcesByServicelDFile Relates services to resources. Maps from ServicelDs to
ResourcelDs for resources belonging to the...

...Maps from Servicell) to Resourcell). DBResourceIDByNameFile Relates the IP names (URLs) of resources to resource **IDs** . 2315 **Maps** from URL to resource ID. DBResourcesByResourcelDFile Relates resources to information sets. Maps Resourcell) to 2317 Resource **Grouplds** .
Servers , Services, IP Information, and Proxies 2W
DBServerIDBylPRIe Relates IP addresses to servers. Maps IP addresses...

...Maps from Servicell) to port number. DBServicelDByServerlDFile Relates servers to ports for services. Maps from **ServerID** to a list of port numbers. DBServicePodToProxyPor1File Relates service pods to the ports for their...

...options data
2301
Fig. 23B
MMF File Name Contents
Access Filter Information 2321
DBAftachedNetworksBylPFile Relates **network** interfaces in the **access** filters to information for the interfaces. Maps from the interface's IP address to interface information. DBAffachedNetworksByServer Relates **access** filters to their **network** interfaces. Maps from IDFile ServerlD for the access filter to interface information. DBRoutingTableFile Describes the...

...2LQ3
DBTrustTableFile Implements the SEND table. Maps from TrustDeflD, indicating
232
a trust level, to **AuthenticationlDs** for **user identification** techniques and EncryptionlDs for encryption techniques.
DBCertificateAuthoritiesFile Relates identifiers for cerfiticate authorities to their data. Maps from CertificateAuthorityll) to associated data. DBTrustAuthenticationsFile Relates AuthenticationlDs to information about **identification**
techniques. **Maps** from AuthenticationlD to **identification** technique information. DBTrustEncryptionsFile Relates EncryptionlDs to information about encryption tech
niques. Maps from Encryptionll) to...

...2623
Fig. 26
POLICY-ENABLED
APPLICATION, -------- ------- POLICY ---------------
2719 POLICY SERVER, 2617
MESSAGES,
2725

---------- POLICY
---------- ----------

@:Aooooaook **SERVER**
NETWORK A DBo 2619
--------- ------- ------------- t
TRAFFIC
BLIC NETWORK, ...011 4009
& AND DestinationPort & destPort
& AND Resource = '" & resource &
& AND IncludeIdentityStore='Y"l
& AND AskClientForIdentities ='Yg"
Set Conn **Server** .CreateObiect("ADODB.Conn.ection")
Set rs = **Server** .CreateObject("ADODB.RecordSet") 4011
Conn.Open dsn, dbuser, dbpass
RS.Open dbsql, Conn @@@ 4013
if...Q LDAP Bind - Neptune
El
Eb- 8YU I C
4RO7
NT Logon Q N T **Logon**
E:@-Q96 **Internet** -4ainternet
E@ 4709
EI-6096 Intranet Internet Sites
Departments
Q I ntranet
El
4805
EiI...

...Q Locations
Q Public Info
El
FIG. 48
LDAPBind Bind to an LDAP Server to **authenticate** a **users** identity 1
(AutoNu
4903 4905 4907
4901
- ------------
344148 Web service proxy
AutoNumber) 0
4911 4913...

...FIG. 50
t
ittp: Hpluto. interdyn. com/B MN eptune. NH
5103
AuUmmUcating WV*b **Server** **User** **ID** : Ifred
Password: 5105
1 n o rd e r to g a i n a...

38/5,K/2 (Item 2 from file: 348)
DIALOG(R)File 348:EUROPEAN PATENTS

01316005
Controlling access to a storage device
Steuerung des Zugriffs auf eine Speicherungsvorrichtung
Controler l'acces a un dispositif de stockage
PATENT ASSIGNEE:
EMC CORPORATION, (2298040), 35 Parkwood Drive, Hopkinton, MA 01748, (US), (Applicant designated States: all)
INVENTOR:
O'Hare, Jeremy, 22 Rocky Woods Road, Hopkinton, Massachussetts 01748, (US)
Kanapathi, Sashe K., 14 Temple Street, Apt. 2E, Framingham, Massachussetts 01702, (US)
LEGAL REPRESENTATIVE:
Freischem, Stephan, Dipl.-Ing. (83231), Patentanwalte Freischem An Gross St. Martin 2, 50667 Koln, (DE)
PATENT (CC, No, Kind, Date): EP 1124172 A2 010816 (Basic)
APPLICATION (CC, No, Date): EP 2001102501 010205;
PRIORITY (CC, No, Date): US 180632 P 000207; US 533009 000322; US 604592 000627; US 774532 010131
DESIGNATED STATES: AT; BE; CH; CY; DE; DK; ES; FI; FR; GB; GR; IE; IT; LI; LU; MC; NL; PT; SE; TR
EXTENDED DESIGNATED STATES: AL; LT; LV; MK; RO; SI
INTERNATIONAL PATENT CLASS: **G06F-001/00** ; G06F-012/14

ABSTRACT EP 1124172 A2
Determining authorization for actions includes defining a plurality of groups, defining a plurality of action types and corresponding levels of authorization for each of the groups, for at least a subset of the action types, defining a plurality of devices on which corresponding actions may be performed, wherein at least some of the devices correspond to portions of a data storage device, and, for the at least one of the groups, determining authorization for a requested action, where if the action corresponds to one of the devices, authorization is determined by examining the levels of authorization for action types corresponding to the at least one group and by examining the plurality of devices corresponding to the requested action and where if the action does not correspond to one of the devices, authorization is determined by examining the levels of authorization for action types corresponding to the at least one group. The action types may include system calls to the data storage device. The at least one of the devices may include at least one disk storage area of the data storage device. The at least one of the devices may include communication ports of the data storage device. The action types may indicate whether system calls are allowed on the communication ports. In response to a requested action being authorized, a tag may be returned that may be used in connection with subsequent requests that the action be performed.
ABSTRACT WORD COUNT: 240
NOTE:
Figure number on first page: 5

LEGAL STATUS (Type, Pub Date, Kind, Text):
Application: 010816 A2 Published application without search report
Change: 030702 A2 Inventor information changed: 20030516
LANGUAGE (Publication,Procedural,Application): English; English; English
FULLTEXT AVAILABILITY:
Available Text Language Update Word Count

CLAIMS A (English) 200133 1781
SPEC A (English) 200133 12695
Total word count - document A 14476
Total word count - document B 0
Total word count - documents A + B 14476

INTERNATIONAL PATENT CLASS: **G06F-001/00** ...

...SPECIFICATION allow restricted access to selected portions of the memory based upon a matrix containing an **ID** for every **host** system that may request access to the memory, an ID for every available memory element, and which types of access each **host ID** is allowed with each memory element. The **requestor ID** number may be created using an existing host computer system hardware **ID** , a **user** password or a group password in a multi-user computer system, a Fibre Channel world wide name, a URL in an **internet access** configuration, a unique random access number assigned by the memory system, a default value, or...host computer system with a hardware ID of 111AAA2, may have 10 terminals and 50 **authorized user** accounts. If all 50 users are permitted by the host system administrator to access every...

38/5,K/3 (Item 3 from file: 348)
DIALOG(R)File 348:EUROPEAN PATENTS

01311001
Controlling access to a storage device
Steuerung des Zugriffs auf eine Speicherungsvorrichtung
Controler l'acces a un dispositif de stockage
PATENT ASSIGNEE:
EMC CORPORATION, (2298040), 35 Parkwood Drive, Hopkinton, MA 01748, (US), (Applicant designated States: all)
INVENTOR:
O'Hare, Jeremy, 2C Country Club Lane, Milford, Massachusetts 01757-2258, (US)
Garrett, Brian, 35 Fruit Street, Hopkinton, MA 01748-1032, (US)
LEGAL REPRESENTATIVE:
Freischem, Stephan, Dipl.-Ing. (83231), Patentanwalte Freischem An Gross St. Martin 2, 50667 Koln, (DE)
PATENT (CC, No, Kind, Date): EP 1122629 A2 010808 (Basic)
APPLICATION (CC, No, Date): EP 2000125969 001128;
PRIORITY (CC, No, Date): US 180632 P 000207; US 533009 000322; US 604592 000627
DESIGNATED STATES: AT; BE; CH; CY; DE; DK; ES; FI; FR; GB; GR; IE; IT; LI; LU; MC; NL; PT; SE; TR
EXTENDED DESIGNATED STATES: AL; LT; LV; MK; RO; SI
INTERNATIONAL PATENT CLASS: **G06F-001/00** ; G06F-012/14

ABSTRACT EP 1122629 A2
Controlling access to a data storage device (W, X, Y, Z) includes defining a plurality of groups (Q, R, S, T, V) that access the data storage device (W, X, Y, Z), defining a plurality of pools of devices of the data storage device (W, X, Y, Z), and, for at least one of the groups (Q, R, S, T, V), determining access rights with respect to at least one of the pools. The pools of devices (W, X, Y, Z) may include communication ports and/or memory segments of the storage element. The access rights may indicate whether system calls are allowed on the communication ports. In some embodiments, restricting access to a data storage device includes coupling each of a plurality of host requestor systems to the storage

element by one of a plurality of ports provided for the storage element and selectively determining, for each of the ports, whether system calls are allowed, where, for the ports in which system calls are not allowed, a system call by the host systems coupled thereto causes the storage element to indicate that the system call was not performed. In other embodiments, the access to pools of memory resources having a unique ID number is restricted to requestors having unique ID numbers in a data base that matches allowed requestors and request types to allowed pools of memory.

ABSTRACT WORD COUNT: 228

NOTE:

Figure number on first page: 5

LEGAL STATUS (Type, Pub Date, Kind, Text):

Application: 010808 A2 Published application without search report

LANGUAGE (Publication,Procedural,Application): English; English; English

FULLTEXT AVAILABILITY:

Available Text	Language	Update	Word Count
CLAIMS A	(English)	200132	1598
SPEC A	(English)	200132	9566
Total word count - document A			11164
Total word count - document B			0
Total word count - documents A + B			11164

INTERNATIONAL PATENT CLASS: **G06F-001/00** ...

...SPECIFICATION allow restricted access to selected portions of the memory based upon a matrix containing an **ID** for every **host** system that may request access to the memory, an ID for every available memory element, and which types of access each **host** **ID** is allowed with each memory element. The **requestor** **ID** number may be created using an existing host computer system hardware **ID** , a **user** password or a group password in a multi-user computer system, a Fibre Channel world wide name, a URL in an **internet** **access** configuration, a unique random access number assigned by the memory system, a default value, or...host computer system with a hardware ID of 111AAA2, may have 10 terminals and 50 **authorized** **user** accounts. If all 50 users are permitted by the host system administrator to access every...

38/5,K/4 (Item 4 from file: 348)

DIALOG(R)File 348:EUROPEAN PATENTS

01311000

Controlling access to a storage device

Steuerung des Zugriffs auf eine Speicherungsvorrichtung

Controler l'acces a un dispositif de stockage

PATENT ASSIGNEE:

EMC CORPORATION, (2298040), 35 Parkwood Drive, Hopkinton, MA 01748, (US), (Applicant designated States: all)

INVENTOR:

O'Hare, Jeremy, 2C Country Club Lane, Milford, Massachusetts 01757-2258, (US)

Garrett, Brian, 35 Fruit Street, Hopkinton, MA 01748-1032, (US)

LEGAL REPRESENTATIVE:

Freischem, Stephan, Dipl.-Ing. (83231), Patentanwalte Freischem An Gross St. Martin 2, 50667 Koln, (DE)

PATENT (CC, No, Kind, Date): EP 1122628 A2 010808 (Basic)

APPLICATION (CC, No, Date): EP 2000125964 001128;

MANAGING IDENTIFICATION IN A DATA COMMUNICATIONS NETWORK
GESTION DE L'IDENTIFICATION DANS UN RESEAU DE COMMUNICATION DE DONNEES

Patent Applicant/Assignee:
SUN MICROSYSTEMS INC, 4120 Network Circle, MS SCA12-203, Santa Clara, CA 95054, US, US (Residence), US (Nationality)
Inventor(s):
DE JONG Eduard K, 522 S. Fremont, San Mateo, CA 94402, US,
LEVY Moshe, 1512 Klamath Drive, Sunnyvale, CA 94087, US,
LEUNG Albert Y, 4175 Orin Court, San Jose, CA 95124, US,
Legal Representative:
RITCHIE David B (et al) (agent), Thelen Reid & Priest LLP, P.O. Box 640640, San Jose, CA 95164-0640, US,

Patent and Priority Information (Country, Number, Date):
Patent: WO 200339095 A2 20030508 (WO 0339095)
Application: WO 2002US34687 20021029 (PCT/WO US0234687)
Priority Application: US 200133373 20011029
Designated States: AE AG AL AM AT AU AZ BA BB BG BR BY BZ CA CH CN CO CR CU CZ DE DK DM DZ EC EE ES FI GB GD GE GH GM HR HU ID IL IN IS JP KE KG KP KR KZ LC LK LR LS LT LU LV MA MD MG MK MN MW MX MZ NO NZ OM PH PL PT RO RU SD SE SG SI SK SL TJ TM TN TR TT TZ UA UG UZ VN YU ZA ZM ZW
(EP) AT BE BG CH CY CZ DE DK EE ES FI FR GB GR IE IT LU MC NL PT SE SK TR
(OA) BF BJ CF CG CI CM GA GN GQ GW ML MR NE SN TD TG
(AP) GH GM KE LS MW MZ SD SL SZ TZ UG ZM ZW
(EA) AM AZ BY KG KZ MD RU TJ TM
Main International Patent Class: **H04L-029/00**
Publication Language: English
Filing Language: English
Fulltext Availability:
Detailed Description
Claims
Fulltext Word Count: 21577

English Abstract
A method for obtaining a service on a data communications network, the method includes enrolling with an authority and using the enrollment results to obtain a service from a service provider. The enrolling creates enrollment results that include user data. The service provider is capable of communicating with the authority to verify the enrollment results.

French Abstract
L'invention concerne un procede permettant d'obtenir un service dans un reseau de communication de donnees. Ce procede consiste a proceder a une inscription aupres d'une autorite et a utiliser les resultats de l'inscription pour obtenir un service aupres d'un fournisseur de service. Cette inscription genere des resultats d'inscription qui comprennent des donnees utilisateur. Le fournisseur de services peut communiquer avec l'autorite afin de verifier les resultats de l'inscription.

Legal Status (Type, Date, Text)
Publication 20030508 A2 Without international search report and to be republished upon receipt of that report.

Main International Patent Class: **H04L-029/00**
Fulltext Availability:
Detailed Description

Detailed Description
... identification server ID and an identification randomized ID. The identification server ID identifies an identification **server** peer **group** . The identification **server** peer **group** includes at least one

server that maintains a **mapping** between an **identification** randomized **ID** and a **user authentication** peer group capable of **authenticating** a **user** associated with a particular randomized **ID** , and a **mapping** between the **identification** randomized **ID** and **user** information. The method also includes requesting **authorization** of the **user** by presenting the **user identifier** to a corresponding **identification server** peer group. Each **server** in the identification **server** peer **group** is configured to search for one or more matching entries including the randomized I]D...Turning now to FIG. 36, a flow diagram that illustrates a method for using federated **identification servers** and federated **user authentication** servers using a randomized **user identifier** to gain access to a service while maintaining privacy in accordance with one embodiment of the present invention is presented. At 3600, a randomized **user identifier** is obtained. At 3605, a determination is made regarding whether it is time to use...

...randomized ID is presented to a service portal. At 3615, a service portal sends a **user authentication** request to the identity server federation that contains the randomized identifier. At 3620, all servers in the identity **server** peer **group** search for a **match** with the randomized **identifier** . At 3625, a determination is made regarding whether a match was found. If there is...a match, at 3635 matching entries from the identity server federation are presented to a **user authentication** server federation to determine a single valid user data entry. Depending upon the amount of **user authentication** required and the capabilities of each **user authentication** server, multiple **user authentication** servers may cooperate in providing the required **user authentication** .

46
[01321 According to one embodiment of the present invention, the federated identity peer group...host 3800.

[01381 Before user 3825 uses service portal 3805 to obtain services on the **Web** , the **user** 3825 must be **authenticated** . This is accomplished by using the **user** identity credential and **authenticated** data in it. This may result in a service credential. User 3 825 issues a service request, includin a **server** group **ID** and the **user** identity credential. The
9
service portal 3805 passes the identity credential to the federated identity server group indicated by the **server** group **ID** to **authenticate** the **user** . The federated identity servers 3 8 1 5 may delegate some or all **user authentication** tasks to federated **user authentication** servers 3820.

48
[01391 According to one embodiment of the present invention, user authentication includes...

38/5,K/7 (Item 7 from file: 349)
DIALOG(R)File 349:PCT FULLTEXT

01008595 **Image available**
ENHANCED PRIVACY PROTECTION IN IDENTIFICATION IN A DATA COMMUNICATIONS NETWORK
PROTECTION DE LA CONFIDENTIALITE RENFORCEE LORS DE L'IDENTIFICATION DANS UN

RESEAU DE TRANSMISSION DE DONNEES

Patent Applicant/Assignee:
SUN MICROSYSTEMS INC, 4120 Network Circle, Santa Clara, CA 95054, US, US (Residence), US (Nationality)
Inventor(s):
DE JONG Eduard K, 522 S. Fremont, San Mateo, CA 94402, US,
LEVY Moshe, 1512 Klamath Drive, Sunnyvale, CA 94087, US,
LEUNG Albert Y, 4175 Orin Court, San Jose, CA 95110, US,
Legal Representative:
RITCHIE David B (et al) (agent), Thelen Reid & Priest LLP, P.O. Box 640640, San Jose, CA 95164-0640, US,

Patent and Priority Information (Country, Number, Date):
Patent: WO 200338580 A2 20030508 (WO 0338580)
Application: WO 2002US34814 20021029 (PCT/WO US0234814)
Priority Application: US 200140270 20011029
Designated States: AE AG AL AM AT AU AZ BA BB BG BR BY BZ CA CH CN CO CR CU CZ DE DK DM DZ EC EE ES FI GB GD GE GH GM HR HU ID IL IN IS JP KE KG KP KR KZ LC LK LR LS LT LU LV MA MD MG MK MN MW MX MZ NO NZ OM PH PL PT RO RU SD SE SG SI SK SL TJ TM TN TR TT TZ UA UG UZ VC VN YU ZA ZM ZW
(EP) AT BE BG CH CY CZ DE DK EE ES FI FR GB GR IE IT LU MC NL PT SE SK TR
(OA) BF BJ CF CG CI CM GA GN GQ GW ML MR NE SN TD TG
(AP) GH GM KE LS MW MZ SD SL SZ TZ UG ZM ZW
(EA) AM AZ BY KG KZ MD RU TJ TM
Main International Patent Class: **G06F-001/00**
Publication Language: English
Filing Language: English
Fulltext Availability:
Detailed Description
Claims
Fulltext Word Count: 21679

English Abstract
A method for enhanced privacy protection in identification in a data communications network includes enrolling for a service on the data communications network, receiving a randomized identifier (ID) in response to the enrolling, storing the randomized ID and using the randomized ID to obtain services on the data communications network. An apparatus for obtaining a service on a data communications network includes an enrollment authority configured to accept an enrollment request. The enrollment authority is further configured to return enrollment results in response to the enrollment request. The enrollment results include user data and the enrollment results may be used obtaining a service from a service provider.

French Abstract
L'invention concerne un procede permettant de renforcer la protection de la confidentialite lors de l'identification dans un reseau de transmission de donnees. Ce procede consiste a s'inscrire a un service sur le reseau de transmission de donnees; a recevoir un identifiant aleatoire (ID) en reponse a l'inscription; a stocker l'identifiant aleatoire, puis a l'utiliser pour obtenir des services sur le reseau de transmission de donnees. L'invention concerne egalement un dispositif permettant d'obtenir un service sur un reseau de transmission de donnees; lequel dispositif comprend une autorite d'inscription configuree pour accepter une demande d'inscription et pour renvoyer les resultats de l'inscription en reponse a la demande d'inscription. Les resultats d'inscription contiennent les donnees utilisateur; ces resultats d'inscription peuvent etre utilises pour obtenir un service chez un prestataire de services.

Legal Status (Type, Date, Text)

Publication 20030508 A2 Without international search report and to be republished upon receipt of that report.
Examination 20030807 Request for preliminary examination prior to end of 19th month from priority date

Main International Patent Class: **G06F-001/00**
Fulltext Availability:
Detailed Description

Detailed Description
... identification server ID and an identification randomized ID. The identification server ID identifies an identification **server** peer **group** . The identification **server** peer **group** includes at least one server that maintains a **mapping** between an **identification** randomized **ID** and a **user authentication** peer group capable of **authenticating** a **user** associated with a particular randomized **ID** , and a **mapping** between the **identification** randomized **ID** and **user** information. The method also includes requesting **authorization** of the **user** by presenting the **user identifier** to a corresponding **identification server** peer group. Each **server** . in the identification **server** peer **group** is configured to search for one or more matching entries including the randomized ID.
[00211...Turning now to FIG. 36, a flow diagram that illustrates a method for using federated **identification servers** and federated **user authentication** servers using a randomized
69
user identifier to gain access to a service while ...in accordance with one embodiment of the present invention is presented. At 3600, a randomized **user identifier** is obtained. At 3605, a determination is made regarding whether it is time to use...

...randomized ID is presented to a service portal. At 3615, a service portal sends a **user authentication** request to the identity server federation that contains the randomized identifier. At 3620, all servers in the identity **server** peer **group** search for a **match** with the randomized **identifier** . At 3625, a detennination is made regarding ...a match, at 3635 matching entries from the identity server federation are presented to a **user authentication** server federation to determine a single valid user data entry. Depending upon the amount of **user authentication** required and the capabilities of each **user authentication** server, multiple **user authentication** servers may cooperate in providing the required **user authentication** .

[0132] According to one embodiment of the present invention, the federated identity peer group is...

38/5,K/8 (Item 8 from file: 349)
DIALOG(R)File 349:PCT FULLTEXT

01008593 **Image available**
USER ACCESS CONTROL TO DISTRIBUTED RESOURCES ON A DATA COMMUNICATIONS NETWORK
CONTROLE D'ACCES UTILISATEUR A DES RESSOURCES REPARTIES SUR UN RESEAU DE TRANSMISSION DE DONNEES
Patent Applicant/Assignee:
SUN MICROSYSTEMS INC, 4120 Network Circle, MS SCA 12-203, Santa Clara, CA 95054, US, US (Residence), -- (Nationality)
Inventor(s):

DE JONG Eduard K, 522 S. Fremont, San Mateo, CA 94402, US,
LEVY Moshe, 1512 Klamath Drive, Sunnyvale, CA 94087, US,
LEUNG Albert Y, 4175 Orin Court, San Jose, CA, US,
Legal Representative:
RITCHIE David B (et al) (agent), Thelen Reid & Priest, LLP, P.O. Box 640640, San Jose, CA, US,
Patent and Priority Information (Country, Number, Date):
Patent: WO 200338578 A2 20030508 (WO 0338578)
Application: WO 2002US34710 20021029 (PCT/WO US0234710)
Priority Application: US 200133373 20011029
Designated States: AE AG AL AM AT AU AZ BA BB BG BR BY BZ CA CH CN CO CR CU CZ DE DK DM DZ EC EE ES FI GB GD GE GH GM HR HU ID IL IN IS JP KE KG KP KR KZ LC LK LR LS LT LU LV MA MD MG MK MN MW MX MZ NO NZ OM PH PL PT RO RU SD SE SG SI SK SL TJ TM TN TR TT TZ UA UG UZ VN YU ZA ZM ZW
(EP) AT BE BG CH CY CZ DE DK EE ES FI FR GB GR IE IT LU MC NL PT SE SK TR
(OA) BF BJ CF CG CI CM GA GN GQ GW ML MR NE SN TD TG
(AP) GH GM KE LS MW MZ SD SL SZ TZ UG ZM ZW
(EA) AM AZ BY KG KZ MD RU TJ TM
Main International Patent Class: **G06F-001/00**
Publication Language: English
Filing Language: English
Fulltext Availability:
Detailed Description
Claims
Fulltext Word Count: 22078

English Abstract
A method for controlling user access to distributed resources on a data communications network includes receiving a resource request. The request includes a rights key credential that includes at least one key to provide access to a resource on the data communications network. The rights key credential also includes a resource identifier that includes a resource server peer group ID and a randomized ID. The resource server peer group ID identifies a resource server peer group. The resource server peer group includes at least one server that maintains a mapping between a randomized ID and the at least one key. The method also includes providing access to the resource using the at least one key.

French Abstract
L'invention concerne un procede permettant de controler l'acces utilisateur a des ressources reparties sur un reseau de transmission de donnees, lequel procede consiste a recevoir une demande de ressources. Cette demande comprend une justification d'identite a cles pour des droits, laquelle contient au moins une cle permettant d'acceder a une ressource sur le reseau de transmission de donnees. La justification d'identite contient egalement un identifiant ressources comprenant une identification de groupe d'homologues serveurs de ressources et une identification aleatoire. L'identification de groupe d'homologues identifie un groupe d'homologues serveurs de ressources, lequel groupe comprend au moins un serveur conservant une application entre une identification aleatoire et ladite cle. Le procede decrit dans cette invention consiste egalement a fournir un acces a des ressources a l'aide de la cle susmentionnee.

Legal Status (Type, Date, Text)
Publication 20030508 A2 Without international search report and to be republished upon receipt of that report.
Examination 20030814 Request for preliminary examination prior to end of 19th month from priority date

Main International Patent Class: **G06F-001/00**

Fulltext Availability:
Detailed Description

Detailed Description
... identification server fD and an identification randomized IID. The identification server ID identifies an identification **server** peer **group** . The identification **server** peer **group** includes at least one server that maintains a **mapping** between an **identification** randomized **ID** and a **user authentication** peer group capable of **authenticating** a **user** associated with a particular randomized **ID** , and a **mapping** between the **identification** randomized] **ID** and **user** information. The method also includes requesting **authorization** of the **user** by presenting the **user identifier** to a corresponding **identification server** peer
Ln
,group. Each **server** in the identification **server** peer **group** is configured to search for one or more matching entries including the randomized BD.

t...Turnincy now to FIG. 36, a flow diaerram that illustrates a method for using federated **identification servers** and federated **user authentication** servers using a randomized **user identifier** to gain access to a service while maintaining privacy in accordance with one embodiment of the present invention is presented. At 3600, a randomized **user identifier** is obtained. At 3605, a determination is made regardinCF whether it is time to use...randomized ID is presented to a service portal. At 3615, a service portal sends a **user authentication** request to the identity server federation that contains the randomized identifier, At 3620, all servers in the identity **server** peer **group** search for a **match** with the randomized **identifier** . At 3625, a determination is made regardiner whether a match
C@ tD
was found. If...

...is a match, at 3635matchincy entries from the identity server federation are presented to a **user authentication** server federation to determine a sincyle valid user data entry. Depending upon the amount of **user authentication** required and the capabilities of each **user authentication** server, multiple **user authentication** servers may cooperate in providing the required **user authentication** .

[01321 According to one embodiment of the present invention, the federated identity peer group is...

38/5,K/9 (Item 9 from file: 349)
DIALOG(R)File 349:PCT FULLTEXT

01008592 **Image available**
PRIVACY AND IDENTIFICATION IN A DATA COMMUNICATION NETWORK
CONFIDENTIALITE ET IDENTIFICATION AU SEIN D'UN RESEAU DE COMMUNICATION DE DONNEES
Patent Applicant/Assignee:
SUN MICROSYSTEMS INC, 4120 Network Circle, MS SCA 12-203, Santa Clara, CA 95054, US, US (Residence), US (Nationality)
Inventor(s):
DE JONG Eduard K, 522 S. Fremont, San Mateo, CA 94402, US,
LEVY Moshe, 1512 Klamath Drive, Sunnyvale, CA 94087, US,
LEUNG Albert Y, 4175 Orin Court, San Jose, CA, US,

Legal Representative:
RITCHIE David B (et al) (agent), Thelen Reid & Priest LLP, P.O. Box 640640, San Jose, CA 95164-0644, US,
Patent and Priority Information (Country, Number, Date):
Patent: WO 200338577 A2 20030508 (WO 0338577)
Application: WO 2002US34709 20021029 (PCT/WO US0234709)
Priority Application: US 200133373 20011029
Designated States: AE AG AL AM AT AU AZ BA BB BG BR BY BZ CA CH CN CO CR CU CZ DE DK DM DZ EC EE ES FI GB GD GE GH GM HR HU ID IL IN IS JP KE KG KP KR KZ LC LK LR LS LT LU LV MA MD MG MK MN MW MX MZ NO NZ OM PH PL PT RO RU SD SE SG SI SK SL TJ TM TN TR TT TZ UA UG UZ VN YU ZA ZM ZW
(EP) AT BE BG CH CY CZ DE DK EE ES FI FR GB GR IE IT LU MC NL PT SE SK TR
(OA) BF BJ CF CG CI CM GA GN GQ GW ML MR NE SN TD TG
(AP) GH GM KE LS MW MZ SD SL SZ TZ UG ZM ZW
(EA) AM AZ BY KG KZ MD RU TJ TM
Main International Patent Class: **G06F-001/00**
Publication Language: English
Filing Language: English
Fulltext Availability:
Detailed Description
Claims
Fulltext Word Count: 22784

English Abstract
A method for managing identification in a data communications network includes receiving a user-controlled secure storage device and enrolling the user with an authority network site. The enrolling includes providing information requested by the authority network site. The method also includes receiving user data in response to the enrolling, storing the user data in the user-controlled secure storage device, enabling the user-controlled secure storage device to release the user data and using the user data at a service provider network site to obtain a service.

French Abstract
Cette invention concerne un procede de gestion de l'identification dans un reseau de communication de donnees, qui consiste a recevoir un dispositif de stockage securise controle par l'utilisateur et a inscrire l'utilisateur aupres d'un site reseau d'autorisation. L'inscription equivaut a fournir des informations demandees par le site reseau d'autorisation. Le procede consiste egalement a recevoir des donnees utilisateur en reponse a l'inscription, a stocker ces donnees utilisateur dans un dispositif de stockage securise controle par l'utilisateur, a autoriser ce dispositif a divulguer les donnees utilisateur et a utiliser ces donnees dans un site reseau de fourniture de services en vue de l'obtention d'un service.

Legal Status (Type, Date, Text)
Publication 20030508 A2 Without international search report and to be republished upon receipt of that report.

Main International Patent Class: **G06F-001/00**
Fulltext Availability:
Detailed Description
Detailed Description
... identification server ID and an identification randomized ID. The identification server ED identifies an identification **server** peer **group** . The identification **server** peer **group** includes at least one server that maintains a **mapping** between an **identification** randomized **ID** and a **user** **authentication** peer group capable of **authenticating** a **user** associated with a particular randomized **ID** , and a **mapping** between the **identification** randomized **ID** and **user** information. The

method also includes requesting **authorization** of the **user** by presenting the **user identifier** to a corresponding **identification server** peer orroup. Each **server** in the identification **server** peer **group** is configured to search for one or more matching entries including the randomized ID.

[00211...

38/5,K/10 (Item 10 from file: 349)
DIALOG(R)File 349:PCT FULLTEXT

01008590 **Image available**
PORTABILITY AND PRIVACY WITH DATA COMMUNICATIONS NETWORK BROWSING
PORTABILITE ET CONFIDENTIALITE DANS L'EXPLORATION D'UN RESEAU DE COMMUNICATION DE DONNEES
Patent Applicant/Assignee:
SUN MICROSYSTEMS INC, 901 San Antonio Road, Palo Alto, CA 94303, US, US (Residence), US (Nationality)
Inventor(s):
DE JONG Eduard K, 522 S. Fremont, San Mateo, CA 94402, US,
LEVY Moshe, 1512 Klamath Drive, Sunnyvale, CA 94087, US,
LEUNG Albert Y, 4175 Orin Court, San Jose, CA 95110, US,
Legal Representative:
RITCHIE David B (et al) (agent), Thelen Reid & Priest LLP, P.O. Box 640640, San Jose, CA 95164-0640, US,
Patent and Priority Information (Country, Number, Date):
Patent: WO 200338575 A2 20030508 (WO 0338575)
Application: WO 2002US34505 20021028 (PCT/WO US0234505)
Priority Application: US 200114934 20011029
Designated States: AE AG AL AM AT AU AZ BA BB BG BR BY BZ CA CH CN CO CR CU CZ DE DK DM DZ EC EE ES FI GB GD GE GH GM HR HU ID IL IN IS JP KE KG KP KR KZ LC LK LR LS LT LU LV MA MD MG MK MN MW MX MZ NO NZ OM PH PL PT RO RU SD SE SG SI SK SL TJ TM TN TR TT TZ UA UG UZ VC VN YU ZA ZM ZW
(EP) AT BE BG CH CY CZ DE DK EE ES FI FR GB GR IE IT LU MC NL PT SE SK TR
(OA) BF BJ CF CG CI CM GA GN GQ GW ML MR NE SN TD TG
(AP) GH GM KE LS MW MZ SD SL SZ TZ UG ZM ZW
(EA) AM AZ BY KG KZ MD RU TJ TM
Main International Patent Class: **G06F-001/00**
Publication Language: English
Filing Language: English
Fulltext Availability:
Detailed Description
Claims
Fulltext Word Count: 22664

English Abstract
A method for browsing a data communications network includes requesting user data from a user-controlled secure device if a network site that requires the user data is accessed. The request is performed prior to requesting the user data from another device. The method also includes sending the user data to a network server associated with the network site if the user data is received from the user-controlled secure device. According to another aspect, a method for servicing data communications network information units includes receiving user data associated with a network site, using the user data if the user data includes static user data and reconstructing the user data before using the user data if the user data includes dynamic user data.

French Abstract
L'invention concerne un procede d'exploration d'un reseau de communication de donnees, consistant a demander des donnees d'utilisateur a un dispositif securise commande par l'utilisateur si un site du reseau exigeant les donnees de l'utilisateur est contacte. La demande est executee avant de demander les donnees d'utilisateur a un autre dispositif. Le procede consiste egalement a envoyer les donnees d'utilisateur a un serveur de reseau associe au site du reseau si les donnees d'utilisateur sont recues du dispositif securise commande par l'utilisateur. Dans un autre aspect, l'invention concerne un procede visant a desservir des unites d'information du reseau de communication de donnees, consistant a recevoir des donnees d'utilisateur associees a un site du reseau, a utiliser les donnees d'utilisateur si les donnees d'utilisateur comprennent des donnees d'utilisateur statiques, et a reconstruire les donnees d'utilisateur avant d'utiliser les donnees d'utilisateur si les donnees d'utilisateur comprennent des donnees d'utilisateur dynamiques.

Legal Status (Type, Date, Text)
Publication 20030508 A2 Without international search report and to be republished upon receipt of that report.

Main International Patent Class: **G06F-001/00**
Fulltext Availability:
Detailed Description

Detailed Description
... server ED and an identification randomized ID. The identification server
8
ID identifies an identification **server** peer **group** . The identification **server** peer **group** includes at least one server that maintains a **mapping** between an **identification** randomized **ID** and a **user authentication** peer group capable of **authenticating** a **user** associated with a particular randomized **ID** , and a **mapping** between the **identification** randomized **ID** and **user** information. The method also includes requesting **authorization** of the **user** by presenting the **user identifier** to a corresponding **identification** server peer group. Each **server** in the identification **server** peer **group** is configured to search for one or more matching entries including the randomized ID. [00211...ling now to FIG. 36, a flow diagram that illustrates a method for using federated **identification servers** and federated **user authentication** servers using a randomized **user identifier** to gain access to a service while maintaining privacy in accordance with one embodiment of the present invention is presented. At 3600, a
64
randomized **user identifier** is obtained. At 3605, a determination is made regarding whether it is time to use...

...randomized ID is presented to a service portal. At 3615, a service portal sends a **user authentication** request to the identity server federation that contains the randomized identifier. At 3620, all servers in the identity **server** peer **group** search for a **match** with the randomized **identifier** . At 3 625, a detennination is made regarding whether a match' was found. If there...

...a match, at 3635 matching entries from the identity server federation are presented to a **user authentication** server federation to determine a single valid user data entry. Depending upon the amount of **user authentication** required and the capabilities of each **user authentication** server, multiple **user authentication** servers may

cooperate in providing the required **user authentication** .
[01321 According to one embodiment of

45/5,K/1 (Item 1 from file: 349)
DIALOG(R)File 349:PCT FULLTEXT

00766325 **Image available**
CRYPTOGRAPHIC REPRESENTATION OF SESSIONS
REPRESENTATION CRYPTOGRAPHIQUE DE SESSIONS
Patent Applicant/Assignee:
THE BRODIA GROUP, Suite 1530, 221 Main Street, San Francisco, CA 94105, US, US (Residence), US (Nationality)
Inventor(s):
RUBIN Paul, Suite 1530, 221 Main Street, San Francisco, CA 94105, US,
GOLDSTEIN Theodore Charles, Suite 1530, 221 Main Street, San Francisco, CA 94105, US,
Legal Representative:
MEYER Virginia (agent), Meyer Intellectual Property Law, Suite 275, 475 Gate Five Road, Sausalito, CA 94965, US,
Patent and Priority Information (Country, Number, Date):
Patent: WO 200079726 A2-A3 20001228 (WO 0079726)
Application: WO 2000US17368 20000621 (PCT/WO US0017368)
Priority Application: US 99338914 19990623
Designated States: AE AL AM AT AT (utility model) AU AZ BA BB BG BR BY CA CH CN CR CU CZ CZ (utility model) DE DE (utility model) DK DK (utility model) DM EE EE (utility model) ES FI FI (utility model) GB GD GE GH GM HR HU ID IL IN IS JP KE KG KP KR KR (utility model) KZ LC LK LR LS LT LU LV MA MD MG MK MN MW MX NO NZ PL PT RO RU SD SE SG SI SK SK (utility model) SL TJ TM TR TT TZ UA UG UZ VN YU ZA ZW
(EP) AT BE CH CY DE DK ES FI FR GB GR IE IT LU MC NL PT SE
(OA) BF BJ CF CG CI CM GA GN GW ML MR NE SN TD TG
(AP) GH GM KE LS MW MZ SD SL SZ TZ UG ZW
(EA) AM AZ BY KG KZ MD RU TJ TM
Main International Patent Class: **H04L-029/06**
Publication Language: English
Filing Language: English
Fulltext Availability:
Detailed Description
Claims
Fulltext Word Count: 4818

English Abstract
A method and system for providing secure access to accounts on a server connected to a computer network. According to the invention, session state information corresponding to a particular account user is encrypted and transmitted to the account user who transmits the encrypted session state information back with each request. When the account user submits a request to the server, the server decrypts the encrypted session state information and validates the session state information. If the session state information is valid, the server processes the user's request. Thus, the user becomes the source of the session state information, albeit in encrypted form, rather than a central database.

French Abstract
L'invention concerne un procede et un systeme permettant de fournir un acces securise aux comptes d'un serveur connecte a un reseau informatique. Selon l'invention, les informations d'etat de session correspondant a un utilisateur de compte donne sont cryptees et transmises a cet utilisateur qui retransmet ces informations avec chaque demande. Lorsque l'utilisateur de compte soumet une demande au serveur, ce dernier decrypte les informations cryptees et les valide. Si lesdites informations sont valables, le serveur traite la demande de l'utilisateur. C'est ainsi l'utilisateur, plutot qu'une base de donnees

centrale, qui devient la source des informations d'etat de session, meme cryptees.

Legal Status (Type, Date, Text)

Publication	20001228	A2 Without international search report and to be republished upon receipt of that report.
Examination	20010329	Request for preliminary examination prior to end of 19th month from priority date
Search Rpt	20010503	Late publication of international search report
Republication	20010503	A3 With international search report.
Republication	20010503	A3 Before the expiration of the time limit for amending the claims and to be republished in the event of the receipt of amendments.

Main International Patent Class: **H04L-029/06**
Fulltext Availability:
Detailed Description

Detailed Description
... illustrates a preferred method of the present invention. The first preferred embodiment contemplates that users **access** the service provider **web** site 80 on client computers 70 over the Internet 60. As is conventional, a user...

...include a 1 0 domain name or may comprises an IP address, consisting of numbers **identifying** the **host** **server** . in preferred form, when the user accesses service provider site 80, the account user is prompted for an account name or **user** **identification** and corresponding password (step 12). Server 50 passes the received account name and password to the master **user** database 40, which **authenticates** the **user** by comparing these inputs to the account 1 5 names and passwords stored in the...
?

```
File 347:JAPIO Oct 1976-2003/Apr(Updated 030804)
         (c) 2003 JPO & JAPIO
File 350:Derwent WPIX 1963-2003/UD,UM &UP=200353
         (c) 2003  Thomson Derwent
? ds

Set     Items   Description
S1     305143   ID OR IDS OR IDENTIFIER? OR IDENTIFIE?
              OR IDENTIFY?
S2      17856   S1(2N)(USER? ? OR ENDUSER? OR SUBSCRIBER? OR REQUEST?R? ? -
             OR MEMBER? ? OR PURCHASER? OR CLIENT? ? OR PARTICIPANT? OR BU-
             YER? ? OR PATRON? ? OR CONSUMER? ? OR CUSTOMER? OR SHOPPER?)
S3         11   USERID? ?
S4       2582   S1(2N)(SERVER? ? OR HOST? ? OR MAINFRAME? OR MAIN()FRAME? ?
              OR RAS) OR SERVERID? ? OR HOSTID? ?
S5     189336   AUTHENTICAT? OR VERIFIE? ? OR VERIFICAT? OR VERIFY? OR VAL-
             IDAT? OR AUTHORIS? OR AUTHORIZ? OR SUBSTANTIAT? OR CONFIRM?
S6      17627   S5(3N)(USER? ? OR ENDUSER? OR SUBSCRIBER? OR REQUEST?R? ? -
             OR MEMBER? ? OR PURCHASER? OR CLIENT? ? OR PARTICIPANT? OR BU-
             YER? ? OR PATRON? ? OR CONSUMER? ? OR CUSTOMER? OR SHOPPER?)
S7     220697   SERVER? ? OR HOST? ? OR MAINFRAME? OR MAIN()FRAME? ?
S8      21341   S7(3N)(GROUP??? ? OR COMMUNAL? OR COLLECTIVE? OR COMMUNITY
             OR SET OR SETS OR NETWORK? OR BLOC OR BLOCS OR BLOCK? ? OR CL-
             USTER? OR SERIES)
S9         49   MULTISERVER? OR MULTIHOST?
S10      2456   (MULTI OR MANY OR SEVERAL OR NUMEROUS OR PLURALIT? OR MULT-
             IPLE OR MULTITUD? OR CHAIN? OR NUMBER)(1W)S7
S11   8187133   ACCESS OR ACCESSE? ? OR ACCESSING OR REACCESS? OR LOGON? OR
              (LOG OR LOGS OR LOGGING)()(ON OR 'IN') OR LOGIN OR USE OR US-
             ES OR USAGE OR USING
S12       618   S2:S3 AND S4
S13       126   S12 AND S6
S14     56472   S11(3N)(NETWORK? ? OR LAN OR LANS OR WAN OR WANS OR NET()W-
             ORK? ? OR EXTRANET? OR INTERNET? OR INTRANET? OR WLAN? ? OR S-
             UBNET? OR VPN? ? OR MULTICOMPUT?)
S15         4   S11(3N)SUB()(NET OR NETS)
S16     13254   S11(3N)(WEB OR WEBSITE? OR WWW OR W3 OR NET OR WEBPAGE?)
S17        38   S13 AND S14:S16
S18     14253   (S1 OR KEY? ?)(3N)(MATCH? OR COMPAR? OR MAP OR MAPS OR MAP-
             PED OR MAPPING?)
S19        14   S13 AND S18
S20        35   S12 AND S8:S10 AND S14:S16
S21         0   S13 AND (MULTIMAP? OR HASHMAP?)
S22        38   S13 AND S14:S16
S23        31   S13 AND S8:S10
S24        16   S12 AND (S8:S10 OR S14:S16) AND (S18 OR MULTIMAP? OR HASHM-
             AP?)
S25        56   S2:S3(20N)S6 AND S4(20N)S6
S26        28   S25 AND (S8:S10 OR S14:S16 OR S18 OR MULTIMAP? OR HASHMAP?)
S27     66878   IC='G06F-001'
S28     45390   IC='H04L-029'
S29        98   S17 OR S19:S24 OR S26
S30        17   S29 AND S27:S28
S31     41768   IC='G06F-015/16':IC='G06F-015/167'
S32        12   S29 AND S31
S33     26841   IC='H04L-009'
S34        15   S29 AND S33
S35      4030   MC='T01-N02B1B'
S36      1999   MC='T01-J12'
S37      6783   MC='W01-A05B'
```

```
S38         16   S29 AND S35:S37
S39         42   (S30 OR S32 OR S34 OR S38) NOT S15
S40         42   IDPAT (sorted in duplicate/non-duplicate order)
S41         41   IDPAT (primary/non-duplicate records only)
? t41/9/1,11

 41/9/1     (Item 1 from file: 350)
DIALOG(R)File 350:Derwent WPIX
(c) 2003  Thomson Derwent. All rts. reserv.

015494851    **Image available**
WPI Acc No: 2003-556998/200352
XRPX Acc No: N03-442632
   User  identification  method in data communication network, involves
  comparing  randomized  ID 's respectively included in received  user
  identifier  and maintained in  identified  server  peer  group  storing
  user information
Patent Assignee: SUN MICROSYSTEMS INC (SUNM  )
Inventor: DE JONG E K; LEUNG A Y; LEVY M
Number of Countries: 101  Number of Patents: 002
Patent Family:
Patent No     Kind   Date    Applicat No    Kind   Date     Week
US 20030084170  A1  20030501  US 200114823    A   20011029  200352  B
WO 200338579   A1  20030508  WO 2002US34713  A   20021029  200352

Priority Applications (No Type Date): US 200114823 A 20011029
Patent Details:
Patent No  Kind Lan Pg   Main IPC    Filing Notes
US 20030084170 A1    76 G06F-015/16
WO 200338579  A1 E     G06F-001/00
   Designated States (National): AE AG AL AM AT AU AZ BA BB BG BR BY BZ CA
   CH CN CO CR CU CZ DE DK DM DZ EC EE ES FI GB GD GE GH GM HR HU ID IL IN
   IS JP KE KG KP KR KZ LC LK LR LS LT LU LV MA MD MG MK MN MW MX MZ NO NZ
   OM PH PL PT RO RU SD SE SG SI SK SL TJ TM TN TR TT TZ UA UG UZ VC VN YU
   ZA ZM ZW
   Designated States (Regional): AT BE BG CH CY CZ DE DK EA EE ES FI FR GB
   GH GM GR IE IT KE LS LU MC MW MZ NL OA PT SD SE SK SL SZ TR TZ UG ZM ZW

Abstract (Basic): US 20030084170 A1
       NOVELTY - A  user  identifier  including an  identification
    server  ID  and an identification randomized ID is obtained. The  user
      identifier  is provided to an  identification  server peer group
    identified using the server  ID  for  authorizing  user  (700) by
    comparing randomized ID's respectively included in the  user
    identifier  and maintained in the  server  peer  group  that also
    stores associated user information.
       DETAILED DESCRIPTION - INDEPENDENT CLAIMS are also included for the
    following:
       (1) program storage device storing  user  identification  program;
    and
       (2)  user  identification  apparatus.
       USE - For  user  identification  in data communication network
    e.g. LAN, WAN, internet, cable television network, telephone network,
    wireless telecommunication network, fiber optic network, ATM network,
    satellite communication network for service provision.
       ADVANTAGE - Performs efficient  user  authentication  using
    received and stored data on open network without revealing unnecessary
    information while maintaining privacy.
       DESCRIPTION OF DRAWING(S) - The figure shows the flow diagram
    illustrating the conduction of secure transactions using  user
```

identification .
user (700)
pp; 76 DwgNo 7/51
Title Terms: USER; IDENTIFY; METHOD; DATA; COMMUNICATE; NETWORK; COMPARE; RANDOM; ID; RESPECTIVE; RECEIVE; USER; IDENTIFY; MAINTAIN; IDENTIFY; SERVE; PEER; GROUP; STORAGE; USER; INFORMATION
Derwent Class: T01; W01
International Patent Class (Main): **G06F-001/00 ; G06F-015/16**
International Patent Class (Additional): **H04L-029/06**
File Segment: EPI
Manual Codes (EPI/S-X): **T01-N02B1B** ; T01-S03; **W01-A05B**

41/9/11 (Item 11 from file: 350)
DIALOG(R)File 350:Derwent WPIX

014779503 **Image available**
WPI Acc No: 2002-600209/200264
XRPX Acc No: N02-475797
Flexible service distribution for large scale communication network has secondary database for recovering user **and** server identifiers **from primary database**
Patent Assignee: PLATA-ANDRES I (PLAT-I); SANCHEZ-HERRERO J (SANC-I); TELEFONAKTIEBOLAGET ERICSSON L M (TELF)
Inventor: PLATA-ANDRES I; SANCHEZ-HERRERO J; ANDRES I P; SANCHEZ HERRERO J A
Number of Countries: 100 Number of Patents: 002
Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Week
WO 200271674	A2	20020912	WO 2002EP2440	A	20020306	200264 B
US 20020147845	A1	20021010	US 2001273759	A	20010306	200269
			US 200291658	A	20020304	

Priority Applications (No Type Date): US 200291658 A 20020304; US 2001273759 P 20010306
Patent Details:

Patent No	Kind	Lan	Pg	Main IPC	Filing Notes
WO 200271674	A2	E	42	H04L-000/00	

Designated States (National): AE AG AL AM AT AU AZ BA BB BG BR BY BZ CA CH CN CO CR CU CZ DE DK DM DZ EC EE ES FI GB GD GE GH GM HR HU ID IL IN IS JP KE KG KP KR KZ LC LK LR LS LT LU LV MA MD MG MK MN MW MX MZ NO NZ OM PH PL PT RO RU SD SE SG SI SK SL TJ TM TN TR TT TZ UA UG UZ VN YU ZA ZM ZW
Designated States (Regional): AT BE CH CY DE DK EA ES FI FR GB GH GM GR IE IT KE LS LU MC MW MZ NL OA PT SD SE SL SZ TR TZ UG ZM ZW

US 20020147845	A1	G06F-015/16	Provisional application US 2001273759	

Abstract (Basic): WO 200271674 A2
NOVELTY - The User Distribution Server (UDS) has a secondary database for recovering **user** and **server identifiers** from the primary database and any other UDS in the network domain. The UDS is located accessible to query and request user information by redirecting the query to the appropriate server or serving entity.
DETAILED DESCRIPTION - Preferably, the User Distribution Server (UDS) has the ability to handle request from other UDS or Service Request Node by indicating that query on the new **identifier** in another **server** is necessary, and optionally indicating the reason behind. INDEPENDENT claims are also included for the following:
(1) A telecommunication system comprising the User Distribution

Server.

(2) A method in a network domain for **identifying** a **user** under different service environments.

USE - For large communication **networks** that **use multiple servers** to provide services to **subscribers** that is **identified** or accessed by a number of different **user identifiers** .

ADVANTAGE - The use of primary and secondary database simplifies data handling as data changes and updates can be easily managed in the primary databases and then transferred to or actualized in the secondary database.

DESCRIPTION OF DRAWING(S) - The drawing shows a network architecture containing the primary and secondary database structure.

pp; 42 DwgNo 1/4

Title Terms: FLEXIBLE; SERVICE; DISTRIBUTE; SCALE; COMMUNICATE; NETWORK; SECONDARY; DATABASE; RECOVER; USER; SERVE; IDENTIFY; PRIMARY; DATABASE

Derwent Class: T01; W01

International Patent Class (Main): **G06F-015/16** ; H04L-000/00

File Segment: EPI

Manual Codes (EPI/S-X): T01-J05B4P; T01-N02A2B; W01-A06B5B

? t41/9/18,21

41/9/18 (Item 18 from file: 350)

DIALOG(R)File 350:Derwent WPIX

014260989 **Image available**

WPI Acc No: 2002-081687/200211

Related WPI Acc No: 2000-223340

XRPX Acc No: N02-060772

Client connection re-establishment method in computer network, involves enabling client to send message to different network address associated with unique identifier **of particular** server

Patent Assignee: INT BUSINESS MACHINES CORP (IBMC)

Inventor: COTNER C L; PICKEL J W

Number of Countries: 001 Number of Patents: 001

Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Week	
US 6247055	B1	20010612	US 96674239	A	19960628	200211	B
			US 98109528	A	19980702		

Priority Applications (No Type Date): US 96674239 A 19960628; US 98109528 A 19980702

Patent Details:

Patent No	Kind	Lan	Pg	Main IPC	Filing Notes
US 6247055	B1		17	G06F-015/16	Div ex application US 96674239 Div ex patent US 6031978

Abstract (Basic): US 6247055 B1

NOVELTY - The client (131) receives an unique identifier assigned to particular server, during initial connection. The client sends a message to any active **server** in the computer **network** , to receive different network address associated with received **identifier** . The **client** sends another message to the different network address, to re-establish connection with the particular server.

DETAILED DESCRIPTION - INDEPENDENT CLAIMS are also included for the following:

(a) Method for re-establishing connection to failed database manufacturing system (DBMS) server;

(b) Method for establishing connection between client server;

(c) System for re-establishing connection to failed DBMS server;

(d) System for establishing connection between client and server;
(e) Computer program product

USE - For enabling a client system networked in sysplex environment through TCP/IP **network** to locate specific **server** . Also for **use** with multiprocessor **network** , file **server** , print **server** , file transfer programs (FTP), etc.

ADVANTAGE - Preserves ability of client to access the sysplex seamlessly. Enhances work load balancing and data availability. Allows two-phase commit protocol to work properly even when DBMS **server** 's **network** attributes are impacted.

DESCRIPTION OF DRAWING(S) - The figure shows the explanatory drawing of sysplex environment.

Client (131)

pp; 17 DwgNo 1/5

Title Terms: CLIENT; CONNECT; ESTABLISH; METHOD; COMPUTER; NETWORK; ENABLE; CLIENT; SEND; MESSAGE; NETWORK; ADDRESS; ASSOCIATE; UNIQUE; IDENTIFY; SERVE

Derwent Class: T01; W01

International Patent Class (Main): **G06F-015/16**

File Segment: EPI

Manual Codes (EPI/S-X): T01-H07C3; T01-H07C5A; T01-H07C5E; T01-H07C5S; T01-H07C7C; T01-J05B2; T01-M02A1B; T01-S03; W01-A06E1; W01-A06F

41/9/21 (Item 21 from file: 350)

DIALOG(R)File 350:Derwent WPIX

014131966 **Image available**

WPI Acc No: 2001-616177/200171

XRPX Acc No: N01-459658

Web site authenticity verification method in electronic commerce, involves comparing **site** identification **included in web page with prestored** identification **at verification** server

Patent Assignee: TRADESAFELY.COM LTD (TRAD-N)

Inventor: HAWKES M E; HAWKES M

Number of Countries: 095 Number of Patents: 005

Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Week	
WO 200163878	A1	20010830	WO 2001GB754	A	20010222	200171	B
EP 1128628	A1	20010829	EP 2000301409	A	20000223	200171	
GB 2359904	A	20010905	GB 20004304	A	20000223	200171	
AU 200135765	A	20010903	AU 200135765	A	20010222	200202	
EP 1260079	A1	20021127	EP 2001907897	A	20010222	200302	
			WO 2001GB754	A	20010222		

Priority Applications (No Type Date): GB 20004304 A 20000223; EP 2000301409 A 20000223

Patent Details:

Patent No	Kind	Lan	Pg	Main IPC	Filing Notes
WO 200163878	A1	E	30	H04L-029/06	

Designated States (National): AE AG AL AM AT AU AZ BA BB BG BR BY BZ CA CH CN CR CU CZ DE DK DM DZ EE ES FI GB GD GE GH GM HR HU ID IL IN IS JP KE KG KP KR KZ LC LK LR LS LT LU LV MA MD MG MK MN MW MX MZ NO NZ PL PT RO RU SD SE SG SI SK SL TJ TM TR TT TZ UA UG US UZ VN YU ZA ZW

Designated States (Regional): AT BE CH CY DE DK EA ES FI FR GB GH GM GR IE IT KE LS LU MC MW MZ NL OA PT SD SE SL SZ TR TZ UG ZW

EP 1128628	A1	E		H04L-029/06	

Designated States (Regional): AL AT BE CH CY DE DK ES FI FR GB GR IE IT LI LT LU LV MC MK NL PT RO SE SI

GB 2359904 A G06F-001/00
AU 200135765 A H04L-029/06 Based on patent WO 200163878
EP 1260079 A1 E H04L-029/06 Based on patent WO 200163878
Designated States (Regional): AL AT BE CH CY DE DK ES FI FR GB GR IE IT LI LT LU LV MC MK NL PT RO SE SI TR

Abstract (Basic): WO 200163878 A1
NOVELTY - A page request is sent to the site to be **authenticated** from the **user** . A web page containing a site identification is generated and forwarded to the **user** . The site **identification** is forwarded to a **verification** server. The **user** is indicated whether or not the site is authentic by **comparing** the site **identification** with prestored identification.
DETAILED DESCRIPTION - INDEPENDENT CLAIMS are also included for the following:
(a) Computer program product;
(b) Web site authenticity verification system;
(c) Web site authenticity verification program
USE - For verifying authenticity of web site in electronic commerce.
ADVANTAGE - The web site authenticity is efficiently verified at every time the **web** site is **accessed** . Hence efficient goods sale through internet is facilitated.
DESCRIPTION OF DRAWING(S) - The figure shows a schematic view of the web site authenticity verification system.
pp; 30 DwgNo 1/4
Title Terms: WEB; SITE; AUTHENTICITY; VERIFICATION; METHOD; ELECTRONIC; COMPARE; SITE; IDENTIFY; WEB; PAGE; IDENTIFY; VERIFICATION; SERVE
Derwent Class: T01; W01
International Patent Class (Main): **G06F-001/00** ; **H04L-029/0**6
File Segment: EPI
Manual Codes (EPI/S-X): T01-E01C; T01-H07C3C; T01-H07C5A; T01-H07C5E; T01-H07C5S; T01-J05A; T01-J12C; T01-S03; W01-A06A; W01-A06B7
? t41/9/29,33

41/9/29 (Item 29 from file: 350)
DIALOG(R)File 350:Derwent WPIX

012866831 **Image available**
WPI Acc No: 2000-038664/200003
XRPX Acc No: N00-029185
Client user authenticating **method for servers connected in internet**
Patent Assignee: EC CUBED INC (ECCU-N)
Inventor: BARTOLOMEOS E; HOQUE F; RENGARAJAN V; WAINGANKAR P
Number of Countries: 022 Number of Patents: 001
Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Week
WO 9956194	A2	19991104	WO 99US9441	A	19990429	200003 B

Priority Applications (No Type Date): US 99283540 A 19990401; US 9883714 P 19980430
Patent Details:

Patent No	Kind	Lan	Pg	Main IPC	Filing Notes
WO 9956194	A2	E	29	G06F-001/00	

Designated States (National): CN IN JP RU
Designated States (Regional): AT BE CH CY DE DK ES FI FR GB GR IE IT LU MC NL PT SE

Abstract (Basic): WO 9956194 A2

NOVELTY - The IP address and uniform resource locator of the second server is stored in the **server** . The data **identifying** the resources like file, documents and web pages is received from the client. The data used in **identification** of second **server** is transmitted to the client so that **user** of **client** is **authenticated** by second server.

DETAILED DESCRIPTION - The specific data is transmitted to the client to enable user to provide **user ID** and password of the user. The state data is generated and transmitted to the client based on received **user ID** and password.

USE - For **authentication** of **client user** by servers connected in distributed computing network like internet. For **authentication** of **user** of **client** like PC, workstation, cellular telephone, pager.

ADVANTAGE - Facilitates **client user** to provide **authentication** data to only one server that is authenticated by **multiple servers** . Eliminates repetitive, tedious **user authentication** process.

DESCRIPTION OF DRAWING(S) - The figure shows flow chart for illustrating **client user authenticating** process.

pp; 29 DwgNo 3/4

Title Terms: CLIENT; USER; AUTHENTICITY; METHOD; SERVE; CONNECT
Derwent Class: T01; T05
International Patent Class (Main): **G06F-001/00**
File Segment: EPI
Manual Codes (EPI/S-X): T01-H07C3E; T01-H07C5A; T01-H07C5E; T05-D01

41/9/33 (Item 33 from file: 350)
DIALOG(R)File 350:Derwent WPIX

011965766 **Image available**
WPI Acc No: 1998-382676/199833
XRPX Acc No: N98-299485

Network **communication system** using **fire-walls for** internet **- has relay server which transmits information in communication path to communication** group **between client and** server

Patent Assignee: HITACHI LTD (HITA)
Number of Countries: 001 Number of Patents: 002
Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Week	
JP 10154118	A	19980609	JP 96312036	A	19961122	199833	B
JP 3253542	B2	20020204	JP 96312036	A	19961122	200211	

Priority Applications (No Type Date): JP 96312036 A 19961122
Patent Details:

Patent No	Kind	Lan	Pg	Main IPC	Filing Notes
JP 10154118	A		10	G06F-013/00	
JP 3253542	B2		10	G06F-013/00	Previous Publ. patent JP 10154118

Abstract (Basic): JP 10154118 A

The system includes a directory server which is connected to network which has several fire walls that limit connection of server. The directory **server** stores **ID** of each computer **using network** , accessible **user ID** and information regarding communication path. When user of accessed client is a legitimate user of the server, information in communication path is searched from ID information of designated server.

A relay server transmits information in communication path to a communication **group** between client and **server** . The directory server and the fire wall communicate mutually using predetermined setting information. The setting information is updated based on predetermined

set condition.
ADVANTAGE - Improves security. Reduces information updation work.
Dwg.1/8

Title Terms: NETWORK; COMMUNICATE; SYSTEM; FIRE; WALL; RELAY; SERVE; TRANSMIT; INFORMATION; COMMUNICATE; PATH; COMMUNICATE; GROUP; CLIENT; SERVE

Derwent Class: T01; W01

International Patent Class (Main): G06F-013/00

International Patent Class (Additional): G06F-015/00; **H04L-009/32** ; H04L-012/66

File Segment: EPI

Manual Codes (EPI/S-X): T01-H07C5; T01-J12C; **W01-A05B** ; W01-A06E1

```
File   2:INSPEC 1969-2003/Aug W2
         (c) 2003 Institution of Electrical Engineers
File   6:NTIS 1964-2003/Aug W3
         (c) 2003 NTIS, Intl Cpyrght All Rights Res
File   8:Ei Compendex(R) 1970-2003/Aug W2
         (c) 2003 Elsevier Eng.  Info. Inc.
File  34:SciSearch(R) Cited Ref Sci 1990-2003/Aug W2
         (c) 2003 Inst for Sci Info
File  35:Dissertation Abs Online 1861-2003/Jul
         (c) 2003 ProQuest Info&Learning
File  65:Inside Conferences 1993-2003/Aug W2
         (c) 2003 BLDSC all rts. reserv.
File  94:JICST-EPlus 1985-2003/Aug W2
         (c)2003 Japan Science and Tech Corp(JST)
File  95:TEME-Technology & Management 1989-2003/Jul W4
         (c) 2003 FIZ TECHNIK
File  99:Wilson Appl. Sci & Tech Abs 1983-2003/Jul
         (c) 2003 The HW Wilson Co.
File 111:TGG Natl.Newspaper Index(SM) 1979-2003/Aug 15
         (c) 2003 The Gale Group
File 144:Pascal 1973-2003/Aug W2
         (c) 2003 INIST/CNRS
File 202:Info. Sci. & Tech. Abs. 1966-2003/Jul 31
         (c) 2003, EBSCO Publishing
File 233:Internet & Personal Comp. Abs. 1981-2003/Jul
         (c) 2003, EBSCO Pub.
File 266:FEDRIP 2003/Jun
        Comp & dist by NTIS, Intl Copyright All Rights Res
File 434:SciSearch(R) Cited Ref Sci 1974-1989/Dec
         (c) 1998 Inst for Sci Info
File 483:Newspaper Abs Daily 1986-2003/Aug 13
         (c) 2003 ProQuest Info&Learning
File 583:Gale Group Globalbase(TM) 1986-2002/Dec 13
         (c) 2002 The Gale Group

Set     Items   Description
S1    2599460   ID OR IDS OR IDENTIFIER? OR IDENTIFIE? ? OR IDENTIFICATION?
              OR IDENTIFY?
S2      19285   S1(2N)(USER? ? OR ENDUSER? OR SUBSCRIBER? OR REQUEST?R? ? -
             OR MEMBER? ? OR PURCHASER? OR CLIENT? ? OR PARTICIPANT? OR BU-
             YER? ? OR PATRON? ? OR CONSUMER? ? OR CUSTOMER? OR SHOPPER?)
S3         35   USERID? ?
S4       3555   S1(2N)(SERVER? ? OR HOST? ? OR MAINFRAME? OR MAIN()FRAME? ?
              OR RAS) OR SERVERID? ? OR HOSTID? ?
S5    2134138   AUTHENTICAT? OR VERIFIE? ? OR VERIFICAT? OR VERIFY? OR VAL-
             IDAT? OR AUTHORIS? OR AUTHORIZ? OR SUBSTANTIAT? OR CONFIRM?
S6      12083   S5(3N)(USER? ? OR ENDUSER? OR SUBSCRIBER? OR REQUEST?R? ? -
             OR MEMBER? ? OR PURCHASER? OR CLIENT? ? OR PARTICIPANT? OR BU-
             YER? ? OR PATRON? ? OR CONSUMER? ? OR CUSTOMER? OR SHOPPER?)
S7     722962   SERVER? ? OR HOST? ? OR MAINFRAME? OR MAIN()FRAME? ?
S8      41776   S7(3N)(GROUP??? ? OR COMMUNAL? OR COLLECTIVE? OR COMMUNITY
             OR SET OR SETS OR NETWORK? OR BLOC OR BLOCS OR BLOCK? ? OR CL-
             USTER? OR SERIES)
S9       2361   MULTISERVER? OR MULTIHOST?
S10      8994   (MULTI OR MANY OR SEVERAL OR NUMEROUS OR PLURALIT? OR MULT-
             IPLE OR MULTITUD? OR CHAIN? OR NUMBER)(1W)S7
S11  13057527   ACCESS OR ACCESSE? ? OR ACCESSING OR REACCESS? OR LOGON? OR
              (LOG OR LOGS OR LOGGING)()(ON OR 'IN') OR LOGIN OR USE OR US-
             ES OR USAGE OR USING
S12        98   S2:S3 AND S4
S13        17   S12 AND S6
S14        17   S12 AND S8:S10
S15    269219   S11(3N)(NETWORK? ? OR LAN OR LANS OR WAN OR WANS OR NET()W-
             ORK? ? OR EXTRANET? OR INTERNET? OR INTRANET? OR WLAN? ? OR S-
             UBNET? OR VPN? ? OR MULTICOMPUT?)
S16        11   S11(3N)SUB()(NET OR NETS)
S17     42053   S11(3N)(WEB OR WEBSITE? OR WWW OR W3 OR NET OR WEBPAGE?)
S18        18   S12 AND S15:S17
```

S19 39 S13:S14 OR S18
S20 4 S19/2002:2003
S21 35 S19 NOT S20
S22 24 RD (unique items)

22/7/1 (Item 1 from file: 2)
DIALOG(R)File 2:INSPEC

7314593 INSPEC Abstract Number: B2002-08-6150M-140, C2002-08-5640-091
Title: Characterizing large DNS traces using graphs
Author(s): Cranor, C.D.; Gansner, E.; Krishnamurthy, B.; Spatscheck, O.
Author Affiliation: AT&T Labs-Res., Florham Park, NJ, USA
Conference Title: Proceedings of the First ACM SIGCOMM Internet Measurement Workshop. UMW 2001 p.55-67
Publisher: ACM, New York, NY, USA
Publication Date: 2001 Country of Publication: USA viii+311 pp.
Material Identity Number: XX-2002-00525
U.S. Copyright Clearance Center Code: ACM1-58113-435-5/01/0011$5.00
Conference Title: Proceedings of ACM SIGCOMM Internet Measurement Workshop 2001
Conference Date: 1-2 Nov. 2001 Conference Location: San Francisco, CA, USA
Language: English Document Type: Conference Paper (PA)
Treatment: Practical (P)
Abstract: The increasing deployment of overlay networks that rely on DNS tricks has led to added interest in examining DNS traffic. In this paper we report on a characterization of DNS traffic gathered over a period of several weeks at Internet gateway routers (IGRs) in the AT&T Common Backbone. The characterization is carried out using several novel techniques to **identify clients** , local DNS servers, and authoritative DNS servers. Our techniques include passive and active measurements, graph-based analysis, examination of outliers, and explicit checks against data obtained from several external sources. Our contribution is the reduction of a very large data set (over 1 Terabyte of raw data) into a significantly smaller representation that is ideally suited for answering protocol-specific semantic queries quickly. After categorizing the addresses, we **use** the **network** aware clustering technique to **group** local DNS **servers** . By juxtaposing the DNS **server clusters** with **clusters** formed by Web clients obtained from a large portal Web site, we determine the distribution of **identified** DNS **servers** in busy **clusters** . A variety of applications are examined ranging from identifying suspected zombies to helping content distribution networks in mapping location of DNS servers. (8 Refs)
Subfile: B C

22/7/4 (Item 4 from file: 2)
DIALOG(R)File 2:INSPEC

5670336 INSPEC Abstract Number: C9710-5620-005
Title: User authentication **in mobile computing environment**
Author(s): Takubo, A.; Ishikawa, M.; Watanabe, T.; Soga, M.; Mizuno, T.
Author Affiliation: Mitsubishi Electr. Corp., Kamakura, Japan
Journal: IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences vol.E80-A, no.7 p.1288-98
Publisher: Inst. Electron. Inf. & Commun. Eng,
Publication Date: July 1997 Country of Publication: Japan
CODEN: IFESEX ISSN: 0916-8508
SICI: 0916-8508(199707)E80A:7L.1288:UAMC;1-G
Material Identity Number: P710-97008
Language: English Document Type: Journal Paper (JP)
Treatment: Theoretical (T)
Abstract: The computers are connected with each other by the network as a result of the progress of technology in the field of the computer and network, and then all of the data to be processed are transferred quickly

and at the real-time through the computer network. However the user can use the computer system at any time, the user must go to the location of the computer system to use the computer resources. The necessities for using the computer system occur anywhere and anytime in spite of the location of the computer system. For this requirement the mobile computing environment (MCE) is expected strongly. In this paper we introduce the model of MCE and discuss the need of the **user authentication** at entering and **logging - in** the **network** in MCE only with a **user ID** . We propose the method of a **user ID** assignment from which a **server ID** can be decided by a simple logical operation. Also, we propose a protocol for a **user authentication** in MCE and discuss the robustness of security against the various attacking on the route. (20 Refs)
Subfile: C

22/7/5 (Item 5 from file: 2)
DIALOG(R)File 2:INSPEC

5587702 INSPEC Abstract Number: B9707-6210L-011, C9707-5640-003
Title: Authentication system of mobile computing environment
Author(s): Takubo, A.; Ishikawa, M.; Watanabe, T.; Soga, H.; Mizuno, T.
Author Affiliation: Comput. Works, Mitsubishi Electr. Corp., Japan
Journal: Reports of the Graduate School of Electronic Science and Technology, Shizuoka University no.18 p.157-65
Publisher: Shizuoka Univ,
Publication Date: March 1997 Country of Publication: Japan
CODEN: SDDHEN ISSN: 0388-5070
SICI: 0388-5070(199703)18L.157:ASMC;1-#
Material Identity Number: H725-97001
Language: Japanese Document Type: Journal Paper (JP)
Treatment: Applications (A); Theoretical (T)
Abstract: The computers are connected with each other by a network as a result of the progress of technology in the field of computers and networks, and then all of the data to be processed are transferred quickly and at real-time through the computer network. However, the user can use the computer system at any time but must go to the location of the computer system to use the computer resources. The necessities for using the computer system can occur anywhere and at anytime in spite of the location of the computer system. For this requirement there are high expectations of the mobile computing environment (MCE). In this paper we introduce the model of a MCE and discuss the need for **user authentication** at entering and logging into the network in the MCE only with a **user ID** . We propose a method of a **user ID** assignment from which a **server ID** can be decided by a simple logical operation. Also, we propose a protocol for **user authentication** in MCE and discuss the robustness of security against the various attacks on the route. (14 Refs)
Subfile: B C

22/7/7 (Item 7 from file: 2)
DIALOG(R)File 2:INSPEC

4866601 INSPEC Abstract Number: A9504-2980-020, B9503-7410-044, C9503-3380D-061
Title: Access control and security for a distributed control system
Author(s): Meyer, J.; Gotz, A.; Klotz, W.D.
Author Affiliation: ESRF, Grenoble, France
Journal: Nuclear Instruments & Methods in Physics Research, Section A (Accelerators, Spectrometers, Detectors and Associated Equipment) vol.352, no.1-2 p.289-92
Publication Date: 15 Dec. 1994 Country of Publication: Netherlands
CODEN: NIMAER ISSN: 0168-9002
U.S. Copyright Clearance Center Code: 0168-9002/94/$07.00
Conference Title: Third International Conference on Accelerator and Large

Experimental Physics Control Systems
Conference Date: 18-23 Oct. 1993 Conference Location: Berlin, Germany
Language: English Document Type: Conference Paper (PA); Journal Paper (JP)
Treatment: Practical (P)
Abstract: The control system of the European Synchrotron Radiation Facility (ESRF) is object-oriented and distributed. Device access is based on the client-server model. To protect sensitive hardware devices an access control and security system has been added. This offers users read, write, super-user or single-user access to hardware objects, families or even whole areas of the facility. A memory-based security database, accessed by an internal control system service, combines device names, access rights, **user** IDs, **group IDs** and **host / network** addresses. **Access** rights must be requested at connection time and are guaranteed by a fast access key mechanism. The paper describes the design and discusses the needs for the implemented access rights and protection possibilities. (3 Refs)
Subfile: A B C

?t22/7/9,12,15,17-18,20,22,24

22/7/9 (Item 9 from file: 2)
DIALOG(R)File 2:INSPEC

04303833 INSPEC Abstract Number: C9301-6130S-048
Title: A service based security architecture for distributed systems
Author(s): Kading, M.
Author Affiliation: Tech. Univ. Berlin, Germany
Conference Title: Architektur von Rechensystemen. 12. GI-ITG-Fachtagung (Architecture of Computing Systems. 12th GI-ITG-Meeting) p.282-93
Editor(s): Jammel, A.
Publisher: Springer-Verlag, Berlin, Germany
Publication Date: 1992 Country of Publication: West Germany ix+369 pp.
ISBN: 3 540 55340 1
Conference Date: 23-25 March 1992 Conference Location: Kiel, Germany
Language: German Document Type: Conference Paper (PA)
Treatment: Practical (P)
Abstract: Important security requirements in distributed computer systems include safeguard of communication, **user identification** , and access control. The article introduces a system security software architecture, realisable with the aid of available services, which meets these requirements. Features of the development environment based on several workstation computers, service computers, networks, and software, are summarised. Central **server authentication , user identification** , object access, function control, and object flow control service tasks aiding realisation of the security architecture are described. Access control is rule based and is defined by a security policy. Advantages of the distributed system security architecture include system-independence, modularity, and easy expandability. (12 Refs)
Subfile: C

22/7/12 (Item 1 from file: 8)
DIALOG(R)File 8:Ei Compendex(R)

06004285 E.I. No: EIP02066855081
Title: Three-party Encrypted Key Exchange without server public-keys
Author: Lin, Chun-Li; Sun, Hung-Min; Steiner, Michael; Hwang, Tzonelih
Corporate Source: Dept. of Comp. Sci. and Info. Eng. National Cheng Kung University, Tainan 701, Taiwan
Source: IEEE Communications Letters v 5 n 12 December 2001. p 497-499
Publication Year: 2001
CODEN: ICLEF6 ISSN: 1089-7798
Language: English
Document Type: JA; (Journal Article) Treatment: T; (Theoretical)
Journal Announcement: 0202W2

Abstract: Three-party key-exchange protocols with password **authentication - clients** share an easy-to-remember password with a trusted server only-are very suitable for applications requiring secure communications between many light-weight clients (end users); it is simply impractical that every two clients share a common secret. In 1995, Steiner, Tsudik and Waidner proposed a realization of such a three-party protocol based on the Encrypted Key Exchange (EKE) protocols. However, their protocol was later demonstrated to be vulnerable to off-line and undetectable on-line guessing attacks. In 2000, Lin, Sun, and Hwang proposed a secure three-party protocol with server public-keys. However, the approach of using server public-keys is not always a satisfactory solution and is impractical for some environments. In this letter, we propose a secure three-party EKE protocol without server public-keys. 9 Refs.

22/7/15 (Item 1 from file: 35)
DIALOG(R)File 35:Dissertation Abs Online

01754971 ORDER NO: AADAA-I9978381
Techniques for supporting service scalability over the Internet
Author: Fei, Zongming
Degree: Ph.D.
Year: 2000
Corporate Source/Institution: Georgia Institute of Technology (0078)
Director: Mostafa H. Ammar
Source: VOLUME 61/07-B OF DISSERTATION ABSTRACTS INTERNATIONAL. PAGE 3683. 145 PAGES
ISBN: 0-599-84255-5

With the explosive growth of the Internet, the number of clients a service needs to handle can potentially be quite large. We identify two approaches to improve the ability of a service to deal with a large number of clients. One is <italic>replication</italic>, in which a server is replicated and distributed across the Internet. Another is <italic>multicast communication</italic>, in which a server delivers information to multiple clients simultaneously.

To deploy these techniques effectively, we have to deal with several important issues. When replication is used, the primary concern is how a client may discover which of the servers is best to use. This is the <italic>server selection</italic> problem. When multicast is used, it satisfies requests of several users at one time and thus, to some extent, sacrifices the special requirements of each individual user. There is a problem of <italic>accommodating individuality</italic> in multicast communication. We address these two issues in this work.

In the case of server selection, we study the issue in both unicast and multicast environments. For the unicast server selection, we target an environment in which servers are distributed across the Internet, and **clients identify servers** using the application-layer anycasting service. We specifically consider replicated web servers, with a goal to minimize clients' response time. The problem of multicast server selection differs from the unicast case in that the load on servers does not directly depend on the number of clients. We define and give solutions to **several** multicast **server** selection problems, aiming at minimizing the total cost of the system. We also study the selection problem of a special kind of multicast servers (called adaptive servers), and propose several methods to improve the performance perceived by the clients.

In the case of accommodating individuality in the multicast communication, we specifically investigate how to provide interactive functions in partitioned multicast video-on-demand systems. We propose an active buffer management scheme that can achieve a high probability of satisfying individual user requirements for interactivity.

22/7/17 (Item 1 from file: 95)
DIALOG(R)File 95:TEME-Technology & Management

01365139 19991104792
Doppelt gemoppelt. Token-basierende Authentisierung
anonym
Network Computing, v55, n23, pp48-52, 1999
Document type: journal article Language: German
Record type: Abstract
ISSN: 1435-2524

ABSTRACT:
Token und die entsprechenden Authentisierungssysteme sind in der Lage, Gruppen von mobilen Anwendern in jeder Remote-Access-Situation sicher und effizient zu identifizieren. Token-Anwendungen verbessern auch das Sicherheitsniveau, indem sie Administrationshierarchien im Netzwerk aufbauen und das klassische Passwort durch Token verstaerken. In einem Test werden das Management, die Sicherheit, Standardtreue und Bedienerfreundlichkeit von folgenden 4 Token-basierenden Authentisierungssystemen bewertet: CryptoAdmin 4.0 von CryptoCard, Ace/Server 3.3.1 von Security Dynamics, VACman 3.5 von Vasco Data Security und SmartGate 2.6a von V-One. Der Test konzentrierte sich auf die Integration in ein bestehendes Netzwerk und analysierte die Schluesselfunktionen Client-Server-Konfiguration und das User-Token-Management. Als Testsieger wurde das Produkt Ace/Server von Security Dynamics ermittelt.

22/7/18 (Item 1 from file: 99)
DIALOG(R)File 99:Wilson Appl. Sci & Tech Abs

2084890 H.W. WILSON RECORD NUMBER: BAST00018583
Webrelay: a multithreaded HTTP relay server
Zhang, Peter;
Dr. Dobb's Journal v. 25 no2 (Feb. 2000) p. 86-96
DOCUMENT TYPE: Feature Article ISSN: 1044-789X

ABSTRACT: The writer discusses webrelay, a freely available multi-threaded HTTP relay server. Webrelay was designed to address the problem faced by legitimate users of a university library. When these users connected directly to the Internet from an off-campus IP address, the vendor web server typically rejected the access request. Webrelay **authenticates clients** to ensure they are legitimate users before connecting them to the vendor web server. The vendor's **server** subsequently **identifies** requests as coming from the relay server itself, which always has a valid IP address or campus-wide **user identification** .

22/7/20 (Item 2 from file: 144)
DIALOG(R)File 144:Pascal

14555848 PASCAL No.: 00-0221933
Achieving non-repudiation of Web based transactions
KALLA M; WONG J S K; MIKLER A R; ELBERT S
Iowa State Univ, Ames IA, United States
Journal: Journal of Systems and Software, 1999, 48 (3) 165-175
ISSN: 0164-1212 CODEN: JSSODM Availability: INIST-18071
No. of Refs.: 25 Refs.
Document Type: P (Serial) ; A (Analytic)
Country of Publication: United States
Language: English

In this paper, we describe our approach to achieve non-repudiation for World Wide Web (WWW) based transactions. We designed and implemented protocols for preparing digital signatures on the server as well as the client machine. In our design, we use the popular Pretty Good Privacy (PGP) software for preparing and verifying digital signatures. The key-contribution is the deployment of a special purpose HTTP server, called signing server, on the client machine to communicate with the WWW browser.

A signing server is specialized to handle digital signatures. This paper discusses the design and implementation of the signing server protocol to achieve non-repudiation transactions in a WWW based employee information system. The technique of deploying special purpose HTTP servers on the client machine has many applications beyond this. It inter-operates with all types of browsers and is an attractive alternative to browser dependent plug-ins.

22/7/22 (Item 2 from file: 233)
DIALOG(R)File 233:Internet & Personal Comp. Abs.

00354194 94NC07-010
DCA's Remote LAN Node
Boardman, Bruce
Network Computing , July 1, 1994 , v5 n8 p98-100, 102+, 4 Page(s)
ISSN: 1046-4468
Company Name: Digital Communications Associates
Product Name: Remote LAN Node
Presents a mixed review of Remote LAN Node v2.0 ($na), a remote access product from Digital Communications Associates (DCA) of Alpharetta, GA (404). Says Remote LAN Node (RLN) has a strong management component and a good Windows client implementation, but is a mediocre performer with a high price. Reveals that RLN functions as a bridge, supports many protocols, and can assign MAC addresses to **user IDs** permanently across **servers** , but its proprietary multiport asynchronous communications board caused significant performance inconsistencies, even hang-ups in testing. Concludes that of the products tested, RLN had the best management strategy for scaling **access** into large **networks** . Includes one photo and a table comparing features. (CH)

22/7/24 (Item 1 from file: 483)
DIALOG(R)File 483:Newspaper Abs Daily

05146132
HP Software Decides Who Should Have Access to Data
American Banker, p 18, col 1
Jul 23, 1998
ISSN: 0002-7561 NEWSPAPER CODE: AB
DOCUMENT TYPE: News; Newspaper
LANGUAGE: English RECORD TYPE: ABSTRACT
LENGTH: Medium (6-18 col inches)

ABSTRACT: Hewlett-Packard Co. has introduced software designed to make it easier to grant secure information access to individuals outside an organization, such as customers, partners, suppliers, and employees. The HP Praesidium **Authorization Server identifies users** and imposes rules for who can have access to data. It can protect content traveling across corporate intranets, extranets, and the Internet. The controls let the World Wide Web be used "for trading and high- value business customers who wish to exchange funds or see if checks have cleared," said Cyndi Nickel, business planning manager of Hewlett-Packard's Internet security operation.
?

NPL
Full text

```
File 696:DIALOG Telecom. Newsletters 1995-2003/Aug 18
         (c) 2003 The Dialog Corp.
File   9:Business & Industry(R) Jul/1994-2003/Aug 15
         (c) 2003 Resp. DB Svcs.
File  15:ABI/Inform(R) 1971-2003/Aug 16
         (c) 2003 ProQuest Info&Learning
File  98:General Sci Abs/Full-Text 1984-2003/Jul
         (c) 2003 The HW Wilson Co.
File 141:Readers Guide 1983-2003/Jul
         (c) 2003 The HW Wilson Co
File 484:Periodical Abs Plustext 1986-2003/Sep W1
         (c) 2003 ProQuest
File 553:Wilson Bus. Abs. FullText 1982-2003/Jul
         (c) 2003 The HW Wilson Co
File 813:PR Newswire 1987-1999/Apr 30
         (c) 1999 PR Newswire Association Inc
File 613:PR Newswire 1999-2003/Aug 18
         (c) 2003 PR Newswire Association Inc
File 635:Business Dateline(R) 1985-2003/Aug 18
         (c) 2003 ProQuest Info&Learning
File 810:Business Wire 1986-1999/Feb 28
         (c) 1999 Business Wire
File 610:Business Wire 1999-2003/Aug 18
         (c) 2003 Business Wire.
File 369:New Scientist 1994-2003/Aug W1
         (c) 2003 Reed Business Information Ltd.
File 370:Science 1996-1999/Jul W3
         (c) 1999 AAAS
File  20:Dialog Global Reporter 1997-2003/Aug 18
         (c) 2003 The Dialog Corp.
File  16:Gale Group PROMT(R) 1990-2003/Aug 15
         (c) 2003 The Gale Group
File  47:Gale Group Magazine DB(TM) 1959-2003/Aug 07
         (c) 2003 The Gale group
File 148:Gale Group Trade & Industry DB 1976-2003/Aug 15
         (c)2003 The Gale Group
File 160:Gale Group PROMT(R) 1972-1989
         (c) 1999 The Gale Group
File 275:Gale Group Computer DB(TM) 1983-2003/Aug 15
         (c) 2003 The Gale Group
File 621:Gale Group New Prod.Annou.(R) 1985-2003/Aug 15
         (c) 2003 The Gale Group
File 624:McGraw-Hill Publications 1985-2003/Aug 18
         (c) 2003 McGraw-Hill Co. Inc
File 634:San Jose Mercury  Jun 1985-2003/Aug 15
         (c) 2003 San Jose Mercury News
File 636:Gale Group Newsletter DB(TM) 1987-2003/Aug 15
         (c) 2003 The Gale Group
File 647:CMP  Computer Fulltext 1988-2003/Jul W3
         (c) 2003 CMP Media, LLC
File 674:Computer News Fulltext 1989-2003/Aug W2
         (c) 2003 IDG Communications
? ds

Set     Items   Description
S1    4604777   ID OR IDS OR IDENTIFIER? OR IDENTIFIE? ? OR IDENTIFICATION?
                OR IDENTIFY?
S2     212449   S1(2N)(USER? ? OR ENDUSER? OR SUBSCRIBER? OR REQUEST?R? ? -
                OR MEMBER? ? OR PURCHASER? OR CLIENT? ? OR PARTICIPANT? OR BU-
                YER? ? OR PATRON? ? OR CONSUMER? ? OR CUSTOMER? OR SHOPPER?)
```

```
S3          699   USERID? ?
S4         9874   S1(2N)(SERVER? ? OR HOST? ? OR MAINFRAME? OR MAIN()FRAME? ?
                  OR RAS) OR SERVERID? ? OR HOSTID? ?
S5      4793527   AUTHENTICAT? OR VERIFIE? ? OR VERIFICAT? OR VERIFY? OR VAL-
                  IDAT? OR AUTHORIS? OR AUTHORIZ? OR SUBSTANTIAT? OR CONFIRM?
S6       234094   S5(3N)(USER? ? OR ENDUSER? OR SUBSCRIBER? OR REQUEST?R? ? -
                  OR MEMBER? ? OR PURCHASER? OR CLIENT? ? OR PARTICIPANT? OR BU-
                  YER? ? OR PATRON? ? OR CONSUMER? ? OR CUSTOMER? OR SHOPPER?)
S7      4137030   SERVER? ? OR HOST? ? OR MAINFRAME? OR MAIN()FRAME? ?
S8       521554   S7(3N)(GROUP??? ? OR COMMUNAL? OR COLLECTIVE? OR COMMUNITY
                  OR SET OR SETS OR NETWORK? OR BLOC OR BLOCS OR BLOCK? ? OR CL-
                  USTER? OR SERIES)
S9         3932   MULTISERVER? OR MULTIHOST?
S10       86325   (MULTI OR MANY OR SEVERAL OR NUMEROUS OR PLURALIT? OR MULT-
                  IPLE OR MULTITUD? OR CHAIN? OR NUMBER)(1W)S7
S11  21319292   ACCESS OR ACCESSE? ? OR ACCESSING OR REACCESS? OR LOGON? OR
                  (LOG OR LOGS OR LOGGING)()(ON OR 'IN') OR LOGIN OR USE OR US-
                  ES OR USAGE OR USING
S12        1274   S2:S3(S)S4
S13         136   S12(S)S6
S14        7938   S2:S3(20N)S6
S15         274   S4(20N)S6
S16         115   S15(S)S14
S17          10   S13(S)S8:S10
S18  21485203   ACCESS OR ACCESSE? ? OR ACCESSING OR REACCESS? OR LOGON? OR
                  LOG OR LOGS OR LOGGING OR LOGIN OR USE OR USES OR USAGE OR U-
                  SING
S19   2289926   S18(3N)(NETWORK? ? OR LAN OR LANS OR WAN OR WANS OR NET()W-
                  ORK? ? OR EXTRANET? OR INTERNET? OR INTRANET? OR WLAN? ? OR S-
                  UBNET? OR VPN? ? OR MULTICOMPUT?)
S20          38   S18(3N)SUB()(NET OR NETS)
S21     1090509   S18(3N)(WEB OR WEBSITE? OR WWW OR W3 OR NET OR WEBPAGE?)
S22          36   S13(S)S19:S21
S23         181   S12(S)S8:S10
S24         174   S12(S)S19:S21
S25         169   S16:S17 OR S20 OR S22
S26       55342   (S1 OR KEY? ?)(3N)(MATCH? OR COMPAR? OR MAP OR MAPS OR MAP-
                  PED OR MAPPING)
S27         704   MULTIMAP? OR HASHMAP?
S28           1   (S13 OR S23:S24)(S)S26:S27
S29         170   S25 OR S28
S30          18   S29/2002:2003
S31         152   S29 NOT S30
S32          98   RD (unique items)
```

? t32/3,k/6,12,17,21-22,26

32/3,K/6 (Item 5 from file: 9)
DIALOG(R)File 9:Business & Industry(R)

1748584 Supplier Number: 01748584 (USE FORMAT 7 OR 9 FOR FULLTEXT)
Gradient Unveils Kerberos Anti-Web Spoofing Technology
(Gradient Technologies introduces WebCrusader 2.0 to prevent Web spoofing; WebCrusader 2.0 claims to foil spoofing attacks by offering two- way, two-level call authentication)
Newsbytes News Network, p N/A
February 25, 1997
DOCUMENT TYPE: Journal (United States)
LANGUAGE: English RECORD TYPE: Fulltext
WORD COUNT: 301

(USE FORMAT 7 OR 9 FOR FULLTEXT)

TEXT:
...same level of certainty from their intranet and extranet Web pages, and applications. "WebCrusader lets **clients verify** the **ID** of the **server** they are connected to," he said, adding that this has got rid of Web spoofing...

32/3,K/12 (Item 5 from file: 15)
DIALOG(R)File 15:ABI/Inform(R)

01720723 03-71713
New design concepts for an intelligent Internet
Kuo, Geng-Sheng; Lin, Jing-Pei
Communications of the ACM v41n11 PP: 93-98 Nov 1998
ISSN: 0001-0782 JRNL CODE: ACM
WORD COUNT: 3734

...TEXT: servers, who have many service instances. It maintains booked service instances, message encryption keys, and **client host identifications** . In addition, it manages service booking and **client authentication** .

There are several advantages of our secure RPC framework. A client host is responsible for...

32/3,K/17 (Item 10 from file: 15)
DIALOG(R)File 15:ABI/Inform(R)

01312550 99-61946
Web spins new communications era
Elgar, Eric
Computer Reseller News n703 PP: 85, 90+ Sep 30, 1996
ISSN: 0893-8377 JRNL CODE: CRN
WORD COUNT: 1570

...TEXT: to limit user access to the corporate infostructure.

The perfect platform enforces security through bidirectional **authentication** in which **clients** and **server** **identify** themselves through unique encrypted certificates and field-level encryption. The added features of user-definable...

32/3,K/21 (Item 14 from file: 15)
DIALOG(R)File 15:ABI/Inform(R)

00865412 95-14804
Lotus Notes thrives in NLM form
Goldberg, Steven
Network World v11n21 PP: 1, 60+ May 23, 1994
ISSN: 0887-7661 JRNL CODE: NWW
WORD COUNT: 1865

...TEXT: Notes databases. During installation, IDs are established for the Notes Administrator and for the new **server** .

The certifier **ID** , in essence, stamps both the **user** **ID** and the **server** **ID** . This unique stamp, or certificate, is the **validation** mechanism that permits **client** -server and server-server communication.

Notes provides two different certification schemes, canonical and hierarchical. In...

32/3,K/22 (Item 15 from file: 15)
DIALOG(R)File 15:ABI/Inform(R)

00728023 93-77244
MDOS System More Secure. Is It More Complacent, Too?
Trowbridge, Dave
Computer Technology Review v12n8 PP: 1-2, 11 Jul 1992
ISSN: 0278-9647 JRNL CODE: CTN
WORD COUNT: 1507

...TEXT: levels of network security in addition to host security. Level 2, the highest, requires a **matching** password and **user** **ID** in the **server** computer's authorization file. Level 1 requires only the **user** **ID** , and Level O is no security at all. These levels are integrated with the host internal security settings, so that privileges granted are the intersection of the set of privileges **authorized** on the **client** (accessing) computer with those on the server (accessed) computer.

RESOURCE CONTROL

All of the MDOS...

32/3,K/26 (Item 1 from file: 813)
DIALOG(R)File 813:PR Newswire

1180861 SFMW01
RSA Encryption Technology Helps Enable Marimba Offer Secure Solution for Internet Software Management, Distribution

DATE: November 5, 1997 16:58 EST WORD COUNT: 727

... a Castanet Transmitter server and Tuner client. In addition, a secure transmission server can be **authenticated** by **subscribers** , enabling a **subscriber** to **identify** the transmitter **host** name.

Using RSA and VeriSign Digital ID technology, a channel developer may digitally sign a...
? t32/3,k/33,38,40,42-44,47

32/3,K/33 (Item 2 from file: 610)
DIALOG(R)File 610:Business Wire

00094635 19990824236B1359 (USE FORMAT 7 FOR FULLTEXT)
National Grocers Association Endorses Concord EFS' E-Com Solution
Business Wire
Tuesday, August 24, 1999 13:55 EDT
JOURNAL CODE: BW LANGUAGE: ENGLISH RECORD TYPE: FULLTEXT
DOCUMENT TYPE: NEWSWIRE
WORD COUNT: 620

...the manufacturer. All transactions are executed
using the latest security techniques, including firewall interfaces,
encryption, **server authentication** , **user ID** 's, password protection, user
profile controls, and restricted exchange of documents between trading partners.

"Electronic...

32/3,K/38 (Item 5 from file: 20)
DIALOG(R)File 20:Dialog Global Reporter

02152593 (USE FORMAT 7 OR 9 FOR FULLTEXT)
INFOTECH BUYLINE
INFOTECH WEEKLY, p21
June 15, 1998
JOURNAL CODE: WIWY LANGUAGE: English RECORD TYPE: FULLTEXT
WORD COUNT: 501

(USE FORMAT 7 OR 9 FOR FULLTEXT)

... Verisign, to offer 128-bit encryption to Lotus Domino Server customers.
Using Verisign's Global **Server IDs** , approved **customers** may use the encryption for intranet, extranet and Internet communications.
The agreement lets **users verify** when their Domino Server is being accessed and has been issued a Global **Server ID** . If the **server** sees this **ID** it boosts encryption to a stronger level.
Until recently the United States Government did not...

32/3,K/40 (Item 2 from file: 16)
DIALOG(R)File 16:Gale Group PROMT(R)

08874391 Supplier Number: 75288799 (USE FORMAT 7 FOR FULLTEXT)

Power In Hand. (Company Business and Marketing)
Wallach, Susan Levi
Sm@rt Partner, v4, n8, p42
Feb 26, 2001
Language: English Record Type: Fulltext
Document Type: Magazine/Journal; Trade
Word Count: 1700

... is a client that, in the ICU implementation, resides on a Palm Pilot VIIx.

The **client** controls **authentication** and security, so the **server** can **identify** the **user** who is logging in. "When you log in for the first time and you need...

32/3,K/42 (Item 4 from file: 16)
DIALOG(R)File 16:Gale Group PROMT(R)
(c) 2003 The Gale Group. All rts. reserv.

07623657 Supplier Number: 63322728 (USE FORMAT 7 FOR FULLTEXT)
Network management packages. (Buyers Guide)
NANCE, BARRY
Government Computer News, v19, n14, p51
June 5, 2000
Language: English Record Type: Fulltext
Article Type: Buyers Guide
Document Type: Tabloid; Trade
Word Count: 1076

... display graphical maps of the network, discover and identify failing network devices, synchronize lists of **authorized user IDs** across **servers** , distribute software updates as well as server and client configurations, detect network intruders or keep...

32/3,K/43 (Item 5 from file: 16)
DIALOG(R)File 16:Gale Group PROMT(R)
(c) 2003 The Gale Group. All rts. reserv.

07361514 Supplier Number: 59222401 (USE FORMAT 7 FOR FULLTEXT)
Security and encryption. (software industry in Japan)
Japan-U.S. Business Report, n361, pNA
Oct, 1999
Language: English Record Type: Fulltext
Document Type: Newsletter; Trade
Word Count: 690

... NEC CORP. on a new Internet security service. By combining VeriSign's OnSite PKI digital **ID** **server** software with NEC's digital certificate verification system, the service will issue digital certificates, **authen**ticate users , encrypt data transmissions and protect online transactions. NEC hopes the new partnership will generate $46...

...applications. Unlike OnSite, which can take more than 10 days to set up digi-tal **IDs** for new **users** , Go Secure! can generate up to a million digital IDs in a few days. It...

...more suitable to replace less-secure, password-based systems for granting large numbers of users **access** to **Web** applications and

extranet/intranet resources.
Targeting the same market segment, newcomer GRADIENT TECHNOLOGIES, INC. has...

32/3,K/44 (Item 6 from file: 16)
DIALOG(R)File 16:Gale Group PROMT(R)

07340507 Supplier Number: 61953692 (USE FORMAT 7 FOR FULLTEXT)
VPN Authentication Moves To LANs -- Alcatel adds RADIUS technology, typically used for remote access, to its switch.(Company Business and Marketing)
Yasin, Rutrell
InternetWeek, p20
April 24, 2000
Language: English Record Type: Fulltext
Document Type: Tabloid; Trade
Word Count: 485

... the user is prompted for a password or other ID. The switch's integrated Radius **client** then **authenticates** the **user** with information stored in the Radius server.
After the **server identifies** the **user** , the switch places the PC into the authorized subnet or zone. The switch also gathers...

32/3,K/47 (Item 9 from file: 16)
DIALOG(R)File 16:Gale Group PROMT(R)

05178512 Supplier Number: 47902887 (USE FORMAT 7 FOR FULLTEXT)
Reining In Remote Access; RADIUS and TACACS compete to bring better control over dial-up access
Dutcher, William
PC Week, p083
August 11, 1997
Language: English Record Type: Fulltext
Document Type: Magazine/Journal; Tabloid; General Trade
Word Count: 1605

... ID and password system. The simplest way to implement remote access is to embed the **user ID** in the access server itself, because the device that controls the modem and the ports also **validates** the **user** .
For example, Cisco Systems Inc.'s 2500 series of remote access **servers** maintain **user IDs** and passwords as part of the system configuration file. The passwords are usually encrypted within...
? t32/3,k/52-53,55-58,68

32/3,K/52 (Item 14 from file: 16)
DIALOG(R)File 16:Gale Group PROMT(R)

04590804 Supplier Number: 46749545 (USE FORMAT 7 FOR FULLTEXT)
Web spins new communications era -- Browser as window to business world levels playing field, spawns new solutions
Computer Reseller News, n703, p85
Sept 30, 1996
Language: English Record Type: Fulltext
Document Type: Magazine/Journal; Trade

Word Count: 2155

... to limit user access to the corporate infostructure.
The perfect platform enforces security through bidirectional **authentication** in which **clients** and **server** **identify** themselves through unique encrypted certificates and field-level encryption. The added features of user-definable...

32/3,K/53 (Item 15 from file: 16)
DIALOG(R)File 16:Gale Group PROMT(R)

04438075 Supplier Number: 46512676 (USE FORMAT 7 FOR FULLTEXT)
Black Sun creates multiuser VRML: CyberHub turns VRML spaces into interactive worlds
InfoWorld, p016
July 1, 1996
Language: English Record Type: Fulltext
Document Type: Magazine/Journal; Trade
Word Count: 301

... issue with VRML... Our biggest file so far is 100KB," Connell said.
CyberHub includes a **user** **identification** **server** to **verify** a **user** 's entry to a site, a motion-tracking database that follows users' actions, and an...

32/3,K/55 (Item 17 from file: 16)
DIALOG(R)File 16:Gale Group PROMT(R)

03880930 Supplier Number: 45578186 (USE FORMAT 7 FOR FULLTEXT)
NETWORK TROUBLESHOOTING
UNIX News, p40
June, 1995
Language: English Record Type: Fulltext
Document Type: Magazine/Journal; Trade
Word Count: 2062

... US users can use PGP (Pretty Good Privacy). The Kerberos system relies on passwords to **authenticate** **users** which only make sense when put together with code at a central Kerberos server. At the client end the application requests that the Kerberos server **verify** the **user** **ID** . The **server** issues users with keys and logs a database of users and their individual keys, so...data is a temporary key for the session and an encrypted ticket. In order to **authenticate** themself, the **user** returns the ticket to the Kerberos server along with an encrypted message coded with the...

...user decrypts with the issued temporary key - their own key is never sent across the **network** from client to **server** , only the temporary one. It should be noted that Kerberos is included in OSF's...

32/3,K/56 (Item 18 from file: 16)
DIALOG(R)File 16:Gale Group PROMT(R)

02211750 Supplier Number: 42881924 (USE FORMAT 7 FOR FULLTEXT)

Remote LAN Manager: Microsoft's Remote Access Server
Network Computing, p28
April, 1992
Language: English Record Type: Fulltext
Document Type: Magazine/Journal; Trade
Word Count: 720

... Issuing RASDIAL servername will initiate the calling sequence. Once connected, the RAS server validates the **UserID** and password, and checks to see if the **user** is **authorized** to **access** the **network** via async. If a callback mode is specified, the server will drop the carrier and...

...user's station, whereas RASDIAL will answer the phone and prompt for validation information. The **UserID** used to connect does not have to be the same as the login **ID** . All **RAS servers** in the same domain share a common user database, so maintaining **multiple servers** is as painless as it is in the regular NETADMIN utility.
Once the connection is...

32/3,K/57 (Item 1 from file: 47)
DIALOG(R)File 47:Gale Group Magazine DB(TM)
(c) 2003 The Gale group. All rts. reserv.

04694374 SUPPLIER NUMBER: 19148196
Digital IDs .(server , client **certificates for data** authentication)
(Technology Information)
Udell, Jon
Byte, v22, n3, p115(3)
March, 1997
ISSN: 0360-5280 LANGUAGE: English RECORD TYPE: Abstract

Digital IDs .(server , client **certificates for data** authentication)
(Technology Information)

32/3,K/58 (Item 2 from file: 47)
DIALOG(R)File 47:Gale Group Magazine DB(TM)
(c) 2003 The Gale group. All rts. reserv.

03384333 SUPPLIER NUMBER: 08174766 (USE FORMAT 7 OR 9 FOR FULL TEXT)
How does Notes handle security? (security features in Lotus Notes work-group software) (related to 'Sky-high Notes')
Steinberg, Don
PC-Computing, v3, n3, p117(2)
March, 1990
ISSN: 0899-1847 LANGUAGE: ENGLISH RECORD TYPE: FULLTEXT; ABSTRACT
WORD COUNT: 908 LINE COUNT: 00070

... and running is straightforward. (See "How Hard Is Notes to Install?" on page 105.) Creating **user** and **server** IDs takes some work because Notes' security features rest on the system's ability to **validate** the **user** . Each **ID** includes public and private encryption keys, for instance, which can generate an electronic signature that...

32/3,K/68 (Item 9 from file: 148)
DIALOG(R)File 148:Gale Group Trade & Industry DB
(c)2003 The Gale Group. All rts. reserv.

08348348 SUPPLIER NUMBER: 17915328 (USE FORMAT 7 OR 9 FOR FULL TEXT)
V-One raises SmartGate. (the Virtual Open Network Environment Corp's SmartGate secure gateway for network servers) (Product Announcement)
Santo, Brian
Electronic Engineering Times, n879, p106(1)
Dec 11, 1995
DOCUMENT TYPE: Product Announcement ISSN: 0192-1541 LANGUAGE: English RECORD TYPE: Fulltext; Abstract
WORD COUNT: 590 LINE COUNT: 00050

...ABSTRACT: the SmartGate client/server application that can be used as a secure gateway on most **network servers** . The program ensures mutual **authentication** by **client** and server to provide a higher level of network security than firewalls or other secure...

...SmartGate server application, after which SmartGate generates a public encryption key that serves as the **client ID** ; **client** and **server authenticate** each other in subsequent sessions, and a random key is generated rather than a new...
? t32/3,k/72,78

32/3,K/72 (Item 2 from file: 275)
DIALOG(R)File 275:Gale Group Computer DB(TM)

01883722 SUPPLIER NUMBER: 17954050 (USE FORMAT 7 OR 9 FOR FULL TEXT)
Remote access headache remedies. (Microscope Security) (Company Business and Marketing)
Gengler, Barbara
INTERNETWORK, v6, n12, pS8(2)
Dec, 1995
LANGUAGE: English RECORD TYPE: Fulltext; Abstract
WORD COUNT: 1395 LINE COUNT: 00119

... the home network is no longer secure.
The basis of all secure remote access is **user identification** . **Host** systems must be able to **identify** a **user** and **verify** their **identification** before the **user** is able to gain **access** to the **network** information. Although many users believe that pass-words alone provide adequate remote access security, truly...

...technologies such as combined encryption with access control mechanisms. Another new technology called two-factor **user authentication** is a process that **identifies** all **users** and assures that only **authorized users** gain **access** to **network** resources.
Security concerns will become even more of an issue as the number of remotely...

32/3,K/78 (Item 2 from file: 636)
DIALOG(R)File 636:Gale Group Newsletter DB(TM)

04012336 Supplier Number: 53200015 (USE FORMAT 7 FOR FULLTEXT)
-MATRANET: MATRAnet presents M>Wall 4.0, the latest version of its high security firewall.
M2 Presswire, pNA
Nov 9, 1998
Language: English Record Type: Fulltext
Document Type: Newswire; Trade

Word Count: 1201

(USE FORMAT 7 FOR FULLTEXT)
TEXT:
...the strong authentication of POP3 and SMTP email protocols. It employs LDAP directories and Radius **identification servers** to manage **authenticated users**0 . Finally, M>Wall 4 includes a 168-bit triple-DES strong encryption module for which...

...up to the application level, for every communication. * Authentication: the M>Wall Card module enables **user identification** with a smartcard. * Encryption -- scrambling of information and data : ensures the confidentiality and integrity of...
...Key, Defender, Digipass or Vasco. M>Wall is also compatible with LDAP and RADIUS type **user authentication** databases. Smartcard solution simplifies **user identification** M>WallCard is the smartcard module of the M>Wall 4.0 firewall that ensures strong **authentication** . It enables **users** in a company to access information on their **intranet** or on the **Extranet using** a personal smartcard containing their **user ID** . Smartcard **authentication** provides a very deep level of security and integrity in a convenient, standard and customizable...

...s extensive expertise and experience, M>Tunnel was developed in complete accordance with the IPSEC **Internet** security protocol. It **uses** 56 to 168-bit keys (DES, Triple DES) to provide strong cryptographic capability. In October...
? t32/3,k/88,93,95,97-98

32/3,K/88 (Item 1 from file: 647)
DIALOG(R)File 647:CMP Computer Fulltext

01214352 CMP ACCESSION NUMBER: INW20000424S0024
VPN Authentication Moves To LANs - Alcatel adds RADIUS technology, typically used for remote access, to its switch
RUTRELL YASIN
INTERNETWEEK, 2000, n 810, PG20
PUBLICATION DATE: 000424
JOURNAL CODE: INW LANGUAGE: English
RECORD TYPE: Fulltext
SECTION HEADING: NEWS & ANALYSIS
WORD COUNT: 489

... the user is prompted for a password or other ID. The switch's integrated Radius **client** then **authenticates** the **user** with information stored in the Radius server.

After the **server identifies** the **user** , the switch places the PC into the authorized subnet or zone. The switch also gathers...

32/3,K/93 (Item 6 from file: 647)
DIALOG(R)File 647:CMP Computer Fulltext

00518028 CMP ACCESSION NUMBER: NWC19920401S2186
Remote LAN Manager: Microsoft's Remote Access Server (Reviewed, Revealed, Revised)
Eric Hall
NETWORK COMPUTING, 1992, n 304 , 28

PUBLICATION DATE: 920401
JOURNAL CODE: NWC LANGUAGE: English
RECORD TYPE: Fulltext
SECTION HEADING: Logging On
WORD COUNT: 721

... Issuing RASDIAL servername will initiate the calling sequence. Once connected, the RAS server validates the **UserID** and password, and checks to see if the **user** is **authorized** to **access** the **network** via async. If a callback mode is specified, the server will drop the carrier and...

...user's station, whereas RASDIAL will answer the phone and prompt for validation information. The **UserID** used to connect does not have to be the same as the login **ID** . All **RAS servers** in the same domain share a common user database, so maintaining **multiple servers** is as painless as it is in the regular NETADMIN utility.
Once the connection is...

32/3,K/95 (Item 1 from file: 674)
DIALOG(R)File 674:Computer News Fulltext

094516
Building wireless apps just got easier
The best tool for giving mobile workers wireless access to a vertical market application is iConverse's Mobile Studio and Interaction Server.
Byline: BARRY NANCE, NETWORK WORLD GLOBAL TEST ALLIANCE
Journal: Network World Page Number: 58
Publication Date: June 25, 2001
Word Count: 3867 Line Count: 398

Text:
... applications. Mobile Application Server is like having IBM's WebSphere or BEA Systems' WebLogic application **server** already **set** up to deliver application data to mobile devices.M-1 Mobile Application Server's components...

... For each wireless message an application wants to transmit to a mobile user, iConverse Interaction **Server identifies** the **user** 's specific device, renders the appropriate response and then dynamically serves the content in a...
... representation of wireless content into device-specific markup language.Out of necessity, Air2Web's Mobile **Internet** Platform **uses** a **Web** -based architecture. Air2Web doesn't distribute its software on CD-ROMs; rather, developers connect to...

... response according to the device characteristics of the wireless device involved in the session. Mobile **Internet** Platform **uses** XML messages to register an application and its objects (which might include style sheets, audio files and predetermined XML messages), register the wireless application dialogs that you design, **identify** wireless **users** and their devices, and carry on dialogs with wireless devices.On one hand, you use... device confirmations. The other Web interfaces store audio files, dialog elements, style sheets, lists of **authorized** wireless **users** and XML files.With AnyDevice's GoAnywhere Platform, your application uses the vendor's device...

... AnyDevice environment.If the application design calls for the use of a

relational database for **user authentication** , AnyDevice requires that it be Oracle Version 8.1.6 or... release a version of Echo that works on non-Windows computers. Within MMC, an administrator **uses** a **Web** site's or virtual directory's Mobility tab on its property sheet to enable or...
... to keep wireless dialogs authentic, private and unmodified in transit.For security, Air2Web's Mobile **Internet** Platform **uses** digital certificates, which you identify when you use Air2Web's DevCenter to create a new...

...on. Aligo's M-1 Mobile Application Server uses the Lightweight Directory Access Protocol for **user authentication** and PKI for data privacy. AnyDevice's GoAnywhere Platform employs an Oracle database for **user authentication** and the Oracle Obfuscation Toolkit to encrypt passwords traveling across a **network** .The iConverse Interaction **Server** relies on SSL and incorporates WTLS to keep data confidential. MobileQ says XMLEdge can encrypt...

... development and run-time platforms. For wireless application development, any computer with a browser for **accessing** the company's **Web** site and a text editor for creating XML will suffice. Mobile Internet Platform works with...

32/3,K/97 (Item 3 from file: 674)
DIALOG(R)File 674:Computer News Fulltext

046883
Eight things to look for in a directory service
Byline: John Allen, Tony Croes, Howard Marks and Josh Penrod
Journal: Network World Page Number: 56
Publication Date: September 18, 1995
Word Count: 592 Line Count: 51

Text:
... 000 users of your WAN. Without a directory service, this requires adding all 3,000 **user IDs** to the new file server. With StreetTalk or Novell, Inc.'s NetWare Directory Services, you...

... the directory tree rather than specific file servers. Not having to add those 3,000 **user IDs** saves lots of time and, hence, money. Here's what to look for in a...

... contain more items, in the form of an inverted tree. File server independence - Users should **log** on to the **network** rather than to a specific file server. Users then only need to know the name of a service or their complete **user ID** to log on from any location on the network. This allows services to move from...
... Third-party vendors should be able to use directory services to store things such as **host** logon **IDs** , program configuration information and other system-specific information. Integrated services and security - Services such as...

... printing, among others, should take advantage of the directory services to provide things such as **user IDs** and addresses. Network services should be tied into a single logon so that different services use one logon to **validate** the **user** . **User access** to the different **network** services should be controlled by information contained in the directory service. X.500 - For those...

32/3,K/98 (Item 4 from file: 674)
DIALOG(R)File 674:Computer News Fulltext

037285
Notes thrives in NLM form
Network World Test Alliance
Byline: Steven Goldberg
Journal: Network World Page Number: 60
Publication Date: May 23, 1994
Word Count: 1708 Line Count: 156

Text:
...Notes databases. During installation, IDs are established for the Notes Administrator and for the new **server** .

The certifier **ID** , in essence, stamps both the **user ID** and the **server ID** . This unique stamp, or certificate, is the **validation** mechanism that permits **client** -server and server-server communication.

Notes provides two different certification schemes, canonical and hierarchical. In...
?

NPL
Software

```
File 256:SoftBase:Reviews,Companies&Prods. 82-2003/Jul
         (c)2003 Info.Sources Inc
? ds

Set     Items   Description
S1       4244   ID OR IDS OR IDENTIFIER? OR IDENTIFIE?
              OR IDENTIFY?
S2        653   S1(2N)(USER? ? OR ENDUSER? OR SUBSCRIBE
              OR MEMBER? ? OR PURCHASER? OR CLIENT? ? OR PARTICIPANT? OR BU-
              YER? ? OR PATRON? ? OR CONSUMER? ? OR CUSTOMER? OR SHOPPER?)
S3         11   USERID? ?
S4         69   S1(2N)(SERVER? ? OR HOST? ? OR MAINFRAME? OR MAIN()FRAME? ?
              OR RAS) OR SERVERID? ? OR HOSTID? ?
S5       5090   AUTHENTICAT? OR VERIFIE? ? OR VERIFICAT? OR VERIFY? OR VAL-
              IDAT? OR AUTHORIS? OR AUTHORIZ? OR SUBSTANTIAT? OR CONFIRM?
S6       1160   S5(3N)(USER? ? OR ENDUSER? OR SUBSCRIBER? OR REQUEST?R? ? -
              OR MEMBER? ? OR PURCHASER? OR CLIENT? ? OR PARTICIPANT? OR BU-
              YER? ? OR PATRON? ? OR CONSUMER? ? OR CUSTOMER? OR SHOPPER?)
S7      27967   SERVER? ? OR HOST? ? OR MAINFRAME? OR MAIN()FRAME? ?
S8       6267   S7(3N)(GROUP??? ? OR COMMUNAL? OR COLLECTIVE? OR COMMUNITY
              OR SET OR SETS OR NETWORK? OR BLOC OR BLOCS OR BLOCK? ? OR CL-
              USTER? OR SERIES)
S9         81   MULTISERVER? OR MULTIHOST?
S10       938   (MULTI OR MANY OR SEVERAL OR NUMEROUS OR PLURALIT? OR MULT-
              IPLE OR MULTITUD? OR CHAIN? OR NUMBER)(1W)S7
S11     57979   ACCESS OR ACCESSE? ? OR ACCESSING OR REACCESS? OR LOGON? OR
               (LOG OR LOGS OR LOGGING)()(ON OR 'IN') OR LOGIN OR USE OR US-
              ES OR USAGE OR USING
S12         9   S2:S3 AND S4
S13         1   S12/2002:2003
S14         8   S12 NOT S13
? t14/7/1,3-8

 14/7/1
DIALOG(R)File 256:SoftBase:Reviews,Companies&Prods.
(c)2003 Info.Sources Inc. All rts. reserv.

02645877          DOCUMENT TYPE:  Company

RF IDeas Inc (645877)
290 Lexington Dr
Buffalo Grove, IL  60089  United States
TELEPHONE:  (847) 870-1723
TOLL FREE TELEPHONE NUMBER:  (866) 439-4884
FAX:  (847) 483-1129
HOMEPAGE:  http://www.RFIDeas.com

RECORD TYPE:  Directory

CONTACT:  Sales Department

ORGANIZATION TYPE:  Corporation
STATUS:  Active

RF IDeas Incorporated, based in Buffalo Grove, Illinois, develops radio
frequency identification (RFID) systems. The company is known for its AIR
ID proximity systems, developed in 1996 and launched commercially in 1998.
Its AIR ID-HID badge product, introduced in 1999, offers long-range and
short-range access features. Also in 1999, the company first offered
customers its  server -based AIR  ID  Enterprise Management Software
product. The firm has developed a Motorola/Indala proximity reader and the
```

Common Logon- **User Identified** , or CLUI (TM), desktop application sharing product. Its pcProxM readers include USB support features. In 2003, the firm announced the RFID1356i, an iCLASS compatible read/right desktop reader and SDK. RF IDeas has formed strategic alliances with Microsoft (R), Novell, HID, Computer Associates, and other companies.

SALES: NA

REVISION DATE: 20030728

14/7/3
DIALOG(R)File 256:SoftBase:Reviews,Companies&Prods.

00125698 DOCUMENT TYPE: Review

PRODUCT NAMES: SiteMinder (699268); GetAccess (671738); ClearTrust SecureControl 4.2 (725358)

TITLE: Authorization Management Tools Emerge
AUTHOR: Radcliff, Deborah
SOURCE: Computerworld, v34 n37 p72(3) Sep 11, 2000
ISSN: 0010-4841
HOMEPAGE: http://www.computerworld.com

RECORD TYPE: Review
REVIEW TYPE: Product Analysis
GRADE: Product Analysis, No Rating

Netegrity's SiteMinder, Entrust Technologies' GetAccess, Securant Technologies' ClearTrust SecureControl 4.2 are new products designed to automate creation and enforcement of user access-level controls for Web-enabled applications. GetAccess is an authorization management system with which users navigate to the Access Server's login screen to access secure resources. Functions supported include user verification, retrieval of profile information, cookie location and transport, cookie encryption, interception of requests and cookie decryption, and session verification through the Registry Server. It also supports transport by the registry **server** of **user ID** , preferences, roles, and application-specific data to the application on the Web server in order to deliver information to the user. A Mobile Proxy Server manages sessions for cookie-free computers, such as wireless devices. SiteMinder, which integrates with popular existing directories and databases, allows users to request protected resources from the Web server. A Web agent retrieves user credentials from the browser and sends them to the SiteMinder policy server, which then authenticates the user. The policy server sends information to the application, which personalizes content according to the specific users' privileges. ClearTrust Secure Control 4.2 simplifies integration by separating content and applications on separate Web servers. A Clear-Trust plug-in enforces access control for resources.

REVISION DATE: 20020830

14/7/4
DIALOG(R)File 256:SoftBase:Reviews,Companies&Prods.

00106257 DOCUMENT TYPE: Review

PRODUCT NAMES: Microsoft Proxy Server (622257)

TITLE: Watching the Gate
AUTHOR: Chernicoff, David Moran, Joseph
SOURCE: Windows Sources, v6 n2 p121(5) Feb 1998
ISSN: 1065-9641
HOMEPAGE: http://www.winsources.com

RECORD TYPE: Review
REVIEW TYPE: Product Analysis
GRADE: Product Analysis, No Rating

Microsoft Proxy Server offers content caching and firewall features, offering an alternative to a traditional firewall. With a proxy server, instead of giving network clients direct Internet access, all actions are routed through a single point. From that one point of control, it is possible to see where all users are going on the Internet, limit which types of sites they can visit, and set rules for how users can transfer files. Microsoft Proxy Server 2.0 is a significantly less expensive solution than a traditional firewall. It offers dynamic packet filtering, which gives the administrator much more control over packets than any other proxy server. However, it still does not bring as much packet control as is possible with a firewall. The proxy server is transparent to the end-user. When an outside Web **server** attempts to **identify** a **client** connection, it gets the proxy **server** 's **ID** . Since the proxy server is the only system that actually communicates over the Internet, it is the only one that has to run TCP/IP. Clients can run TCP/IP if desired, but they can also run a different network protocol, such as IPX/SPX. It includes a content caching server, which caches the content of user requests from the Internet to a local cache. Proxy Server can be run from any machine with Windows NT Server 4.0, Service Pack 3, and IIS 3.0.

REVISION DATE: 20020630

14/7/5

00100199 DOCUMENT TYPE: Review

PRODUCT NAMES: DB2 2.1.1 (701866); Informix Dynamic Server 7.12 (493619); Microsoft SQL Server (259748); Oracle 7 7.3 (004233); Sybase SQL Server 11 (695017)

TITLE: Database Security
AUTHOR: Rennhackkamp, Martin
SOURCE: DBMS, v10 n2 p67(5) Feb 1997
ISSN: 1041-5173
HOMEPAGE: http://www.dbmsmag.com

RECORD TYPE: Review
REVIEW TYPE: Product Analysis
GRADE: Product Analysis, No Rating

IBM's DB2 2.1.1, Informix Software's Informix-OnLine Dynamic Server 7.12, Microsoft's Microsoft SQL Server, Oracle's Oracle 7 7.3, and Sybase's Sybase SQL Server 11 are compared for their security controls. DB2 2.1.1 has three levels of security checks for viewing or maneuvering stored data; they include system entry, database connection, and database object usage.

Users must be **identified** by a **user** name and password, and privileges are granted with the GRANT statement. Privileges can be granted to individuals, groups, or PUBLIC (all users). Informix-OnLine Dynamic Server 7.12 also uses privileges to grant permission for access, altering, or removal of database objects or the content of database objects. Privileges are granted with the GRANT statement and removed with the REVOKE statement. Connect, resource, and database administration levels are supported. Roles can be used to grant privileges of many users concurrently. Informix-OnLine/Secure Dynamic Server is a licensed component for secure UNIX and CMW platforms, supporting required access controls, systemwide discrete privileges, labeled data, and an audit trail method. Microsoft SQL **Server identifies users** via an administrator-created login ID or one assigned automatically from existing registered Windows NT users. Oracle 7 7.3 has a list of valid users with unique user names and passwords, and SQL Server 11 **users** are also **identified** by unique IDs with passwords.

REVISION DATE: 20030428

14/7/6
DIALOG(R)File 256:SoftBase:Reviews,Companies&Prods.

00091327 DOCUMENT TYPE: Review

PRODUCT NAMES: Novell Directory Services (NDS) 4.1 (460354); GroupWise (709255)

TITLE: NetWare, GroupWise alleviate vitamin company's LAN woe
AUTHOR: Karon, Paul
SOURCE: InfoWorld, v18 n19 p70(1) May 6, 1996
ISSN: 0199-6649
HOMEPAGE: http://www.infoworld.com

RECORD TYPE: Review
REVIEW TYPE: Product Analysis
GRADE: Product Analysis, No Rating

A chain of retail vitamin and supplement stores enjoys tremendous growth, although maintaining the LAN for the chain's 2,500 stores proved to be a complex matter. Administrators turned to Novell's Novell Directory Services (NDS) along with Novell's Groupwise groupware to maintain its rapidly growing LAN. Through NDS, the company has been able to unify their NetWare directories as well as GroupWise directories, providing major time savings for support staff and delivering extended functionality to all end-users. From the end user's point of view, the convenience of single logons and other features make NDS a beneficial application. Before deploying NetWare 4.1, employees had to have different **user IDs** for each **server** . With NetWare 4.1, the IS group was able to create a group object that automatically gave staff members access rights to as many servers as are in the entire WAN environment.

REVISION DATE: 20020630

14/7/7
DIALOG(R)File 256:SoftBase:Reviews,Companies&Prods.

00085131 DOCUMENT TYPE: Review

PRODUCT NAMES: Novell Directory Services (NDS) (460354); StreetTalk (264351); Microsoft Windows NT (347973); cc:Mail (016699); Network Information Service+ (NIS+) (437867)

TITLE: Needle Hunting
AUTHOR: Korzeniowski, Paul
SOURCE: Byte, v20 n11 p51(3) Nov 1995
ISSN: 0360-5280
HOMEPAGE: http://www.byte.com

RECORD TYPE: Review
REVIEW TYPE: Product Analysis
GRADE: Product Analysis, No Rating

The key to effective network management is a good directory system that can **identify users , servers** , and other resources. Novell's NetWare network operating system now includes NetWare Directory Service (NDS), a service similar to Banyan Systems' VINES feature, StreetTalk. NetWare previously supported only basic directory services with the bindery, which stored addressing information on one standalone server. StreetTalk automatically transmits changes to multiple servers. Microsoft is also planning to offer global capabilities in the next release of Windows NT. Lotus Development offers sophisticated directory services with its cc:Mail product. cc:Mail includes the Automatic Directory Exchange feature, which automatically updates all cc:Mail user addresses. Sun Microsystems' Network Information Services Plus directory service, which is bundled with several UNIX operating systems, uses a treelike hierarchical directory structure.

REVISION DATE: 20030527

14/7/8
DIALOG(R)File 256:SoftBase:Reviews,Companies&Prods.

00078248 DOCUMENT TYPE: Review

PRODUCT NAMES: Kane Security Analyst 2.0 (568678)

TITLE: NetWare security tool moves into enterprise
AUTHOR: Krill, Paul
SOURCE: InfoWorld, v17 n22 p45(1) May 29, 1995
ISSN: 0199-6649
HOMEPAGE: http://www.infoworld.com

RECORD TYPE: Review
REVIEW TYPE: Product Analysis
GRADE: Product Analysis, No Rating

Kane Security Analyst 2.0 for UNIX, Windows NT, and NetWare supports security assessment software for the enterprise. The product, a graphical software tool, looks at networks and creates reports about security, including data integrity, confidentiality, user access control, system monitoring, and account limitations. The product also supports NetWare Directory Services (NDS), which enables security analysis by looking at the full network directory tree and all NDS objects. One user, a large manufacturing company, welcomes heterogeneous support via a single, unified interface for all systems. The product evaluates **user** and group **IDs** , **servers** , and containers, as well as NDS objects, for exposure to hackers

and inappropriate security privileges.

REVISION DATE: 20020630
?

```
File 347:JAPIO Oct 1976-2003/Apr(Updated 030804)
         (c) 2003 JPO & JAPIO
File 350:Derwent WPIX 1963-2003/UD,UM &UP=200352
         (c) 2003  Thomson Derwent
File 348:EUROPEAN PATENTS 1978-2003/Jul W03
         (c) 2003 European Patent Office
File 349:PCT FULLTEXT 1979-2002/UB=20030807,UT=20030731
         (c) 2003 WIPO/Univentio
? ds

Set     Items   Description
S1         12   AU='DE JONG E'
S2         43   AU='DE JONG EDUARD':AU='DE JONG EDUARD KAREL'
S3          3   AU='DEJONG E'
S4        199   AU='LEVY M':AU='LEVY M W'
S5         19   AU='LEVY MOSHE':AU='LEVY MOSHE SUN MICROSYSTEMS INC'
S6         17   AU='LEUNG A'
S7          2   AU='LEUNG A Y'
S8          9   AU='LEUNG ALBERT':AU='LEUNG ALBERT M'
S9          1   PA='SUN  RESEARCH AND DEVELOP (SUNO  )'
S10        49   PA='SUN -':PA='SUN -N'
S11         4   PA='SUN MICRO KK':PA='SUN MICRO SYSTEMS INC'
S12      8831   PA='SUN MICROSYST INC':PA='SUN MICROYSTEMS INC'
S13         1   PA='SUN MIRCROSYSTEMS INC'
S14        12   S1:S3 AND S4:S8
S15        30   S1:S8 AND S9:S13
S16     10143   (ID OR IDENTIFIE? OR IDENTIFIC? OR IDENTIFY?)(3N)SERVER? ?
S17         6   S14 AND S16
S18         7   S15 AND S16
S19         7   S17:S18
? t19/9

 19/9/1     (Item 1 from file: 350)
DIALOG(R)File 350:Derwent WPIX
(c) 2003  Thomson Derwent. All rts. reserv.

015494851    **Image available**
WPI Acc No: 2003-556998/200352
XRPX Acc No: N03-442632
  User identification method in data communication network, involves
  comparing randomized ID's respectively included in received user
  identifier and maintained in  identified   server  peer group storing
  user information
Patent Assignee:  SUN MICROSYSTEMS INC  (SUNM
Inventor: DE JONG E K;  LEUNG A Y ;  LEVY M
Number of Countries: 101  Number of Patents: 002
Patent Family:
Patent No     Kind   Date    Applicat No    Kind   Date     Week
US 20030084170  A1  20030501  US 200114823    A   20011029  200352  B
WO 200338579   A1  20030508  WO 2002US34713  A   20021029  200352

Priority Applications (No Type Date): US 200114823 A 20011029
Patent Details:
Patent No  Kind Lan Pg   Main IPC    Filing Notes
US 20030084170 A1    76 G06F-015/16
WO 200338579  A1 E     G06F-001/00
   Designated States (National): AE AG AL AM AT AU AZ BA BB BG BR BY BZ CA
   CH CN CO CR CU CZ DE DK DM DZ EC EE ES FI GB GD GE GH GM HR HU ID IL IN
   IS JP KE KG KP KR KZ LC LK LR LS LT LU LV MA MD MG MK MN MW MX MZ NO NZ
   OM PH PL PT RO RU SD SE SG SI SK SL TJ TM TN TR TT TZ UA UG UZ VC VN YU
   ZA ZM ZW
```

Designated States (Regional): AT BE BG CH CY CZ DE DK EA EE ES FI FR GB GH GM GR IE IT KE LS LU MC MW MZ NL OA PT SD SE SK SL SZ TR TZ UG ZM ZW

Abstract (Basic): US 20030084170 A1

NOVELTY - A user **identifier** including an **identification server ID** and an **identification** randomized ID is obtained. The user identifier is provided to an **identification server** peer group **identified** using the **server ID** for authorizing user (700) by comparing randomized ID's respectively included in the user identifier and maintained in the server peer group that also stores associated user information.

DETAILED DESCRIPTION - INDEPENDENT CLAIMS are also included for the following:

(1) program storage device storing user identification program; and

(2) user identification apparatus.

USE - For user identification in data communication network e.g. LAN, WAN, internet, cable television network, telephone network, wireless telecommunication network, fiber optic network, ATM network, satellite communication network for service provision.

ADVANTAGE - Performs efficient user authentication using received and stored data on open network without revealing unnecessary information while maintaining privacy.

DESCRIPTION OF DRAWING(S) - The figure shows the flow diagram illustrating the conduction of secure transactions using user identification.

user (700)

pp; 76 DwgNo 7/51

Title Terms: USER; IDENTIFY; METHOD; DATA; COMMUNICATE; NETWORK; COMPARE; RANDOM; ID; RESPECTIVE; RECEIVE; USER; IDENTIFY; MAINTAIN; IDENTIFY; SERVE; PEER; GROUP; STORAGE; USER; INFORMATION

Derwent Class: T01; W01

International Patent Class (Main): G06F-001/00; G06F-015/16

International Patent Class (Additional): H04L-029/06

File Segment: EPI

Manual Codes (EPI/S-X): T01-N02B1B; T01-S03; W01-A05B

? t19/5/2-7

19/5/2 (Item 1 from file: 349)

DIALOG(R)File 349:PCT FULLTEXT

01009060 **Image available**

MANAGING IDENTIFICATION IN A DATA COMMUNICATIONS NETWORK

GESTION DE L'IDENTIFICATION DANS UN RESEAU DE COMMUNICATION DE DONNEES

Patent Applicant/Assignee:

SUN MICROSYSTEMS INC , 4120 Network Circle, MS SCA12-203, Santa Clara, CA 95054, US, US (Residence), US (Nationality

Inventor(s):

DE JONG Eduard K , 522 S. Fremont, San Mateo, CA 94402, US,

LEVY Moshe , 1512 Klamath Drive, Sunnyvale, CA 94087, US,

LEUNG Albert Y, 4175 Orin Court, San Jose, CA 95124, US

Legal Representative:

RITCHIE David B (et al) (agent), Thelen Reid & Priest LLP, P.O. Box 640640, San Jose, CA 95164-0640, US,

Patent and Priority Information (Country, Number, Date):

Patent: WO 200339095 A2 20030508 (WO 0339095)

Application: WO 2002US34687 20021029 (PCT/WO US0234687)

Priority Application: US 200133373 20011029

Designated States: AE AG AL AM AT AU AZ BA BB BG BR BY BZ CA CH CN CO CR CU

CZ DE DK DM DZ EC EE ES FI GB GD GE GH GM HR HU ID IL IN IS JP KE KG KP
KR KZ LC LK LR LS LT LU LV MA MD MG MK MN MW MX MZ NO NZ OM PH PL PT RO
RU SD SE SG SI SK SL TJ TM TN TR TT TZ UA UG UZ VN YU ZA ZM ZW
(EP) AT BE BG CH CY CZ DE DK EE ES FI FR GB GR IE IT LU MC NL PT SE SK TR
(OA) BF BJ CF CG CI CM GA GN GQ GW ML MR NE SN TD TG
(AP) GH GM KE LS MW MZ SD SL SZ TZ UG ZM ZW
(EA) AM AZ BY KG KZ MD RU TJ TM
Main International Patent Class: H04L-029/00
Publication Language: English
Filing Language: English
Fulltext Availability:
Detailed Description
Claims
Fulltext Word Count: 21577

English Abstract
A method for obtaining a service on a data communications network, the method includes enrolling with an authority and using the enrollment results to obtain a service from a service provider. The enrolling creates enrollment results that include user data. The service provider is capable of communicating with the authority to verify the enrollment results.

French Abstract
L'invention concerne un procede permettant d'obtenir un service dans un reseau de communication de donnees. Ce procede consiste a proceder a une inscription aupres d'une autorite et a utiliser les resultats de l'inscription pour obtenir un service aupres d'un fournisseur de service. Cette inscription genere des resultats d'inscription qui comprennent des donnees utilisateur. Le fournisseur de services peut communiquer avec l'autorite afin de verifier les resultats de l'inscription.

Legal Status (Type, Date, Text)
Publication 20030508 A2 Without international search report and to be republished upon receipt of that report.

19/5/3 (Item 2 from file: 349)
DIALOG(R)File 349:PCT FULLTEXT

01008595 **Image available**
ENHANCED PRIVACY PROTECTION IN IDENTIFICATION IN A DATA COMMUNICATIONS NETWORK
PROTECTION DE LA CONFIDENTIALITE RENFORCEE LORS DE L'IDENTIFICATION DANS UN RESEAU DE TRANSMISSION DE DONNEES
Patent Applicant/Assignee:
SUN MICROSYSTEMS INC , 4120 Network Circle, Santa Clara, CA 95054, US, US (Residence), US (Nationality
Inventor(s):
DE JONG Eduard K , 522 S. Fremont, San Mateo, CA 94402, US,
LEVY Moshe , 1512 Klamath Drive, Sunnyvale, CA 94087, US,
LEUNG Albert Y, 4175 Orin Court, San Jose, CA 95110, US
Legal Representative:
RITCHIE David B (et al) (agent), Thelen Reid & Priest LLP, P.O. Box 640640, San Jose, CA 95164-0640, US,
Patent and Priority Information (Country, Number, Date):
Patent: WO 200338580 A2 20030508 (WO 0338580)
Application: WO 2002US34814 20021029 (PCT/WO US0234814)
Priority Application: US 200140270 20011029
Designated States: AE AG AL AM AT AU AZ BA BB BG BR BY BZ CA CH CN CO CR CU

CZ DE DK DM DZ EC EE ES FI GB GD GE GH GM HR HU ID IL IN IS JP KE KG KP
KR KZ LC LK LR LS LT LU LV MA MD MG MK MN MW MX MZ NO NZ OM PH PL PT RO
RU SD SE SG SI SK SL TJ TM TN TR TT TZ UA UG UZ VC VN YU ZA ZM ZW
(EP) AT BE BG CH CY CZ DE DK EE ES FI FR GB GR IE IT LU MC NL PT SE SK TR
(OA) BF BJ CF CG CI CM GA GN GQ GW ML MR NE SN TD TG
(AP) GH GM KE LS MW MZ SD SL SZ TZ UG ZM ZW
(EA) AM AZ BY KG KZ MD RU TJ TM
Main International Patent Class: G06F-001/00
Publication Language: English
Filing Language: English
Fulltext Availability:
Detailed Description
Claims
Fulltext Word Count: 21679

English Abstract
A method for enhanced privacy protection in identification in a data communications network includes enrolling for a service on the data communications network, receiving a randomized identifier (ID) in response to the enrolling, storing the randomized ID and using the randomized ID to obtain services on the data communications network. An apparatus for obtaining a service on a data communications network includes an enrollment authority configured to accept an enrollment request. The enrollment authority is further configured to return enrollment results in response to the enrollment request. The enrollment results include user data and the enrollment results may be used obtaining a service from a service provider.

French Abstract
L'invention concerne un procede permettant de renforcer la protection de la confidentialite lors de l'identification dans un reseau de transmission de donnees. Ce procede consiste a s'inscrire a un service sur le reseau de transmission de donnees; a recevoir un identifiant aleatoire (ID) en reponse a l'inscription; a stocker l'identifiant aleatoire, puis a l'utiliser pour obtenir des services sur le reseau de transmission de donnees. L'invention concerne egalement un dispositif permettant d'obtenir un service sur un reseau de transmission de donnees; lequel dispositif comprend une autorite d'inscription configuree pour accepter une demande d'inscription et pour renvoyer les resultats de l'inscription en reponse a la demande d'inscription. Les resultats d'inscription contiennent les donnees utilisateur; ces resultats d'inscription peuvent etre utilises pour obtenir un service chez un prestataire de services.

Legal Status (Type, Date, Text)
Publication 20030508 A2 Without international search report and to be republished upon receipt of that report.
Examination 20030807 Request for preliminary examination prior to end of 19th month from priority date

19/5/4 (Item 3 from file: 349)
DIALOG(R)File 349:PCT FULLTEXT

01008594 **Image available**
ENHANCED QUALITY OF IDENTIFICATION IN A DATA COMMUNICATIONS NETWORK
AMELIORATION DE LA QUALITE D'IDENTIFICATION DANS UN RESEAU DE TRANSMISSION DE DONNEES
Patent Applicant/Assignee:
SUN MICROSYSTEMS INC , 4120 Network Circle, Santa Clara, CA 95054, US,

US (Residence), US (Nationality
Inventor(s):
DE JONG Eduard K , 522 S. Fremont, San Mateo, CA 94402, US,
LEVY Moshe , 1512 Klamath Drive, Sunnyvale, CA 94087, US,
LEUNG Albert Y, 4175 Orin Court, San Jose, CA 95110, US
Legal Representative:
RITCHIE David B (et al) (agent), Thelen Reid & Priest LLP, P.O. Box 640640, San Jose, CA 95164-0640, US,
Patent and Priority Information (Country, Number, Date):
Patent: WO 200338579 A1 20030508 (WO 0338579)
Application: WO 2002US34713 20021029 (PCT/WO US0234713)
Priority Application: US 200114823 20011029
Designated States: AE AG AL AM AT AU AZ BA BB BG BR BY BZ CA CH CN CO CR CU CZ DE DK DM DZ EC EE ES FI GB GD GE GH GM HR HU ID IL IN IS JP KE KG KP KR KZ LC LK LR LS LT LU LV MA MD MG MK MN MW MX MZ NO NZ OM PH PL PT RO RU SD SE SG SI SK SL TJ TM TN TR TT TZ UA UG UZ VC VN YU ZA ZM ZW
(EP) AT BE BG CH CY CZ DE DK EE ES FI FR GB GR IE IT LU MC NL PT SE SK TR
(OA) BF BJ CF CG CI CM GA GN GQ GW ML MR NE SN TD TG
(AP) GH GM KE LS MW MZ SD SL SZ TZ UG ZM ZW
(EA) AM AZ BY KG KZ MD RU TJ TM
Main International Patent Class: G06F-001/00
International Patent Class: H04L-029/06
Publication Language: English
Filing Language: English
Fulltext Availability:
Detailed Description
Claims
Fulltext Word Count: 21515

English Abstract
A method for enhanced quality of identification in a data communications network includes obtaining a user identifier that includes an **identification server ID** and an **identification** randomized **ID** . The **identification server ID identifies** an **identification server** peer group. The **identification server** peer group includes at least one server that maintains a mapping between an identification randomized ID and a user authentication peer group capable of authenticating a user associated with a particular randomized ID, and a mapping between the identification randomized ID and user information. The method also includes requesting authorization of the user by presenting the user identifier to a corresponding **identification server** peer group. Each **server** in the **identification server** peer group is configured to search for one or more matching entries including the randomized ID.

French Abstract
L'invention porte sur un procede ameliorant la qualite d'identification dans un reseau de transmission de donnees consistant a obtenir un identificateur d'utilisateur comprenant un ID d'identification de serveur et un ID d'identification pris au hasard. L'ID d'identification de serveur identifie un groupe de serveurs prestataires de services comportant au moins un serveur contenant: une correspondance entre l'ID d'identification pris au hasard et un groupe pair d'identification de l'utilisateur pouvant authentifier un utilisateur associe a un ID d'identification pris au hasard particulier, et une correspondance entre l'ID d'identification pris au hasard et une information utilisateur. Le procede consiste egalement a requerir l'autorisation de l'utilisateur en presentant l'identificateur d'utilisateur a un groupe de serveurs pairs d'identification correspondant. Chacun des serveurs dudit groupe est concu pour rechercher une ou plusieurs occurrences correspondantes dont l'ID pris au hasard.

Legal Status (Type, Date, Text)
Publication 20030508 A1 With international search report.
Examination 20030710 Request for preliminary examination prior to end of 19th month from priority date

19/5/5 (Item 4 from file: 349)
DIALOG(R)File 349:PCT FULLTEXT

01008593 **Image available**
USER ACCESS CONTROL TO DISTRIBUTED RESOURCES ON A DATA COMMUNICATIONS NETWORK
CONTROLE D'ACCES UTILISATEUR A DES RESSOURCES REPARTIES SUR UN RESEAU DE TRANSMISSION DE DONNEES
Patent Applicant/Assignee:
SUN MICROSYSTEMS INC , 4120 Network Circle, MS SCA 12-203, Santa Clara, CA 95054, US, US (Residence), -- (Nationality
Inventor(s):
DE JONG Eduard K , 522 S. Fremont, San Mateo, CA 94402, US,
LEVY Moshe , 1512 Klamath Drive, Sunnyvale, CA 94087, US,
LEUNG Albert Y, 4175 Orin Court, San Jose, CA, US
Legal Representative:
RITCHIE David B (et al) (agent), Thelen Reid & Priest, LLP, P.O. Box 640640, San Jose, CA, US,
Patent and Priority Information (Country, Number, Date):
Patent: WO 200338578 A2 20030508 (WO 0338578)
Application: WO 2002US34710 20021029 (PCT/WO US0234710)
Priority Application: US 200133373 20011029
Designated States: AE AG AL AM AT AU AZ BA BB BG BR BY BZ CA CH CN CO CR CU CZ DE DK DM DZ EC EE ES FI GB GD GE GH GM HR HU ID IL IN IS JP KE KG KP KR KZ LC LK LR LS LT LU LV MA MD MG MK MN MW MX MZ NO NZ OM PH PL PT RO RU SD SE SG SI SK SL TJ TM TN TR TT TZ UA UG UZ VN YU ZA ZM ZW
(EP) AT BE BG CH CY CZ DE DK EE ES FI FR GB GR IE IT LU MC NL PT SE SK TR
(OA) BF BJ CF CG CI CM GA GN GQ GW ML MR NE SN TD TG
(AP) GH GM KE LS MW MZ SD SL SZ TZ UG ZM ZW
(EA) AM AZ BY KG KZ MD RU TJ TM
Main International Patent Class: G06F-001/00
Publication Language: English
Filing Language: English
Fulltext Availability:
Detailed Description
Claims
Fulltext Word Count: 22078

English Abstract
A method for controlling user access to distributed resources on a data communications network includes receiving a resource request. The request includes a rights key credential that includes at least one key to provide access to a resource on the data communications network. The rights key credential also includes a resource identifier that includes a resource **server** peer group **ID** and a randomized **ID** . The resource **server** peer group **ID** **identifies** a resource **server** peer group. The resource server peer group includes at least one server that maintains a mapping between a randomized ID and the at least one key. The method also includes providing access to the resource using the at least one key.

French Abstract
L'invention concerne un procede permettant de controler l'acces

utilisateur a des ressources reparties sur un reseau de transmission de donnees, lequel procede consiste a recevoir une demande de ressources. Cette demande comprend une justification d'identite a cles pour des droits, laquelle contient au moins une cle permettant d'acceder a une ressource sur le reseau de transmission de donnees. La justification d'identite contient egalement un identifiant ressources comprenant une identification de groupe d'homologues serveurs de ressources et une identification aleatoire. L'identification de groupe d'homologues identifie un groupe d'homologues serveurs de ressources, lequel groupe comprend au moins un serveur conservant une application entre une identification aleatoire et ladite cle. Le procede decrit dans cette invention consiste egalement a fournir un acces a des ressources a l'aide de la cle susmentionnee.

Legal Status (Type, Date, Text)
Publication 20030508 A2 Without international search report and to be republished upon receipt of that report.

19/5/6 (Item 5 from file: 349)
DIALOG(R)File 349:PCT FULLTEXT

01008592 **Image available**
PRIVACY AND IDENTIFICATION IN A DATA COMMUNICATION NETWORK
CONFIDENTIALITE ET IDENTIFICATION AU SEIN D'UN RESEAU DE COMMUNICATION DE DONNEES
Patent Applicant/Assignee:
SUN MICROSYSTEMS INC , 4120 Network Circle, MS SCA 12-203, Santa Clara, CA 95054, US, US (Residence), US (Nationality
Inventor(s):
DE JONG Eduard K , 522 S. Fremont, San Mateo, CA 94402, US,
LEVY Moshe , 1512 Klamath Drive, Sunnyvale, CA 94087, US,
LEUNG Albert Y, 4175 Orin Court, San Jose, CA, US
Legal Representative:
RITCHIE David B (et al) (agent), Thelen Reid & Priest LLP, P.O. Box 640640, San Jose, CA 95164-0644, US,
Patent and Priority Information (Country, Number, Date):
Patent: WO 200338577 A2 20030508 (WO 0338577)
Application: WO 2002US34709 20021029 (PCT/WO US0234709)
Priority Application: US 200133373 20011029
Designated States: AE AG AL AM AT AU AZ BA BB BG BR BY BZ CA CH CN CO CR CU CZ DE DK DM DZ EC EE ES FI GB GD GE GH GM HR HU ID IL IN IS JP KE KG KP KR KZ LC LK LR LS LT LU LV MA MD MG MK MN MW MX MZ NO NZ OM PH PL PT RO RU SD SE SG SI SK SL TJ TM TN TR TT TZ UA UG UZ VN YU ZA ZM ZW
(EP) AT BE BG CH CY CZ DE DK EE ES FI FR GB GR IE IT LU MC NL PT SE SK TR
(OA) BF BJ CF CG CI CM GA GN GQ GW ML MR NE SN TD TG
(AP) GH GM KE LS MW MZ SD SL SZ TZ UG ZM ZW
(EA) AM AZ BY KG KZ MD RU TJ TM
Main International Patent Class: G06F-001/00
Publication Language: English
Filing Language: English
Fulltext Availability:
Detailed Description
Claims
Fulltext Word Count: 22784

English Abstract
A method for managing identification in a data communications network includes receiving a user-controlled secure storage device and enrolling the user with an authority network site. The enrolling includes providing

information requested by the authority network site. The method also includes receiving user data in response to the enrolling, storing the user data in the user-controlled secure storage device, enabling the user-controlled secure storage device to release the user data and using the user data at a service provider network site to obtain a service.

French Abstract
Cette invention concerne un procede de gestion de l'identification dans un reseau de communication de donnees, qui consiste a recevoir un dispositif de stockage securise controle par l'utilisateur et a inscrire l'utilisateur aupres d'un site reseau d'autorisation. L'inscription equivaut a fournir des informations demandees par le site reseau d'autorisation. Le procede consiste egalement a recevoir des donnees utilisateur en reponse a l'inscription, a stocker ces donnees utilisateur dans un dispositif de stockage securise controle par l'utilisateur, a autoriser ce dispositif a divulguer les donnees utilisateur et a utiliser ces donnees dans un site reseau de fourniture de services en vue de l'obtention d'un service.

Legal Status (Type, Date, Text)
Publication 20030508 A2 Without international search report and to be republished upon receipt of that report.

19/5/7 (Item 6 from file: 349)
DIALOG(R)File 349:PCT FULLTEXT

01008590 **Image available**
PORTABILITY AND PRIVACY WITH DATA COMMUNICATIONS NETWORK BROWSING
PORTABILITE ET CONFIDENTIALITE DANS L'EXPLORATION D'UN RESEAU DE COMMUNICATION DE DONNEES
Patent Applicant/Assignee:
SUN MICROSYSTEMS INC , 901 San Antonio Road, Palo Alto, CA 94303, US, US (Residence), US (Nationality
Inventor(s):
DE JONG Eduard K , 522 S. Fremont, San Mateo, CA 94402, US,
LEVY Moshe , 1512 Klamath Drive, Sunnyvale, CA 94087, US,
LEUNG Albert Y, 4175 Orin Court, San Jose, CA 95110, US
Legal Representative:
RITCHIE David B (et al) (agent), Thelen Reid & Priest LLP, P.O. Box 640640, San Jose, CA 95164-0640, US,
Patent and Priority Information (Country, Number, Date):
Patent: WO 200338575 A2 20030508 (WO 0338575)
Application: WO 2002US34505 20021028 (PCT/WO US0234505)
Priority Application: US 200114934 20011029
Designated States: AE AG AL AM AT AU AZ BA BB BG BR BY BZ CA CH CN CO CR CU CZ DE DK DM DZ EC EE ES FI GB GD GE GH GM HR HU ID IL IN IS JP KE KG KP KR KZ LC LK LR LS LT LU LV MA MD MG MK MN MW MX MZ NO NZ OM PH PL PT RO RU SD SE SG SI SK SL TJ TM TN TR TT TZ UA UG UZ VC VN YU ZA ZM ZW
(EP) AT BE BG CH CY CZ DE DK EE ES FI FR GB GR IE IT LU MC NL PT SE SK TR
(OA) BF BJ CF CG CI CM GA GN GQ GW ML MR NE SN TD TG
(AP) GH GM KE LS MW MZ SD SL SZ TZ UG ZM ZW
(EA) AM AZ BY KG KZ MD RU TJ TM
Main International Patent Class: G06F-001/00
Publication Language: English
Filing Language: English
Fulltext Availability:
Detailed Description
Claims
Fulltext Word Count: 22664

English Abstract
A method for browsing a data communications network includes requesting user data from a user-controlled secure device if a network site that requires the user data is accessed. The request is performed prior to requesting the user data from another device. The method also includes sending the user data to a network server associated with the network site if the user data is received from the user-controlled secure device. According to another aspect, a method for servicing data communications network information units includes receiving user data associated with a network site, using the user data if the user data includes static user data and reconstructing the user data before using the user data if the user data includes dynamic user data.

French Abstract
L'invention concerne un procede d'exploration d'un reseau de communication de donnees, consistant a demander des donnees d'utilisateur a un dispositif securise commande par l'utilisateur si un site du reseau exigeant les donnees de l'utilisateur est contacte. La demande est executee avant de demander les donnees d'utilisateur a un autre dispositif. Le procede consiste egalement a envoyer les donnees d'utilisateur a un serveur de reseau associe au site du reseau si les donnees d'utilisateur sont recues du dispositif securise commande par l'utilisateur. Dans un autre aspect, l'invention concerne un procede visant a desservir des unites d'information du reseau de communication de donnees, consistant a recevoir des donnees d'utilisateur associees a un site du reseau, a utiliser les donnees d'utilisateur si les donnees d'utilisateur comprennent des donnees d'utilisateur statiques, et a reconstruire les donnees d'utilisateur avant d'utiliser les donnees d'utilisateur si les donnees d'utilisateur comprennent des donnees d'utilisateur dynamiques.
Legal Status (Type, Date, Text)
Publication 20030508 A2 Without international search report and to be republished upon receipt of that report.
?